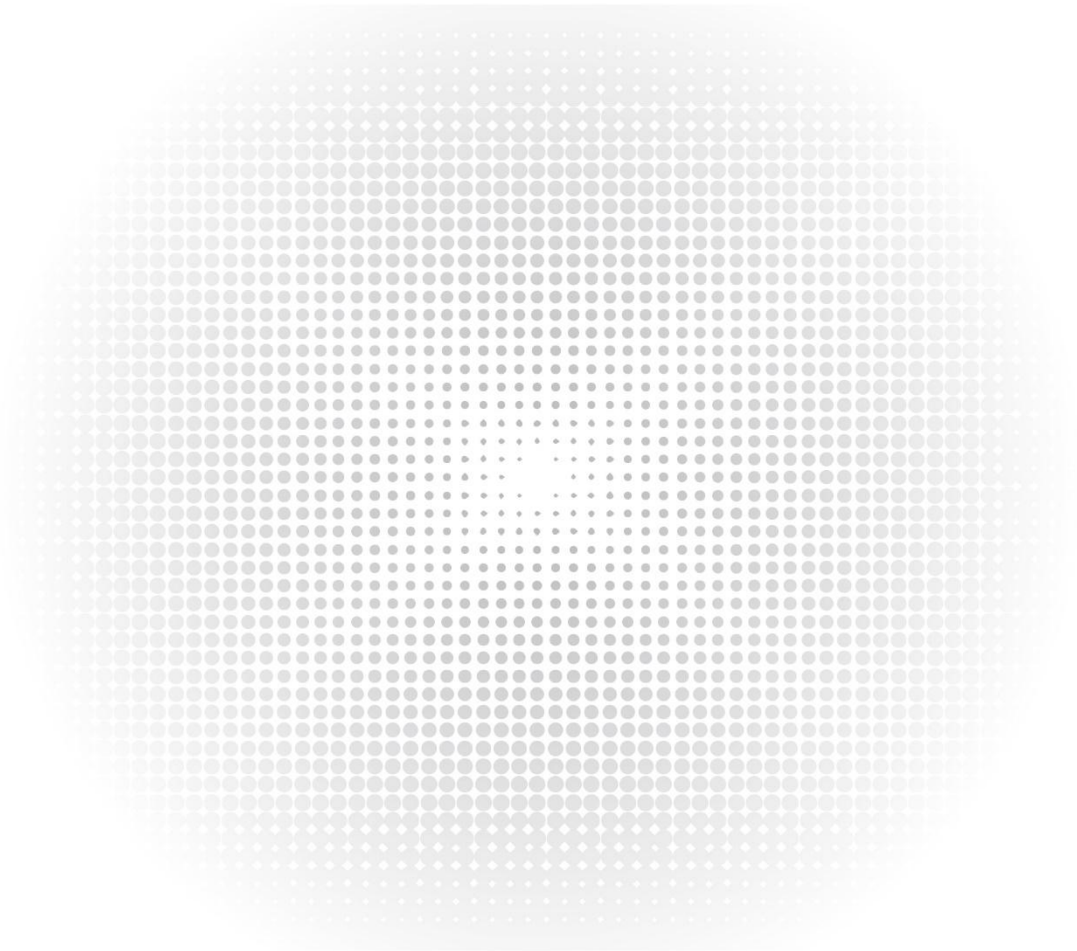
S2805S-48T4S Switch Command Line Interface Reference Guide

Model: S2805S-48T4S



Configuration Guide

Contents

Chapter 1 Fundamentals of system operation 1

1.1 Basic configuration commands for system operation 1

1.1.1 enable 1

1.1.2 end 1

1.1.3 configure terminal 2

1.1.4 exit 2

1.1.5 quit 3

1.1.6 help 4

1.1.7 Shortcut key 5

Chapter 2 Login control and management 8

2.1 Login control and management configuration commands 8

2.1.1 login-access-list telnet 8

2.1.2 login-access-list ssh 8

2.1.3 login-access-list snmp 9

2.1.4 login-access-list web 10

2.1.5 no login-access-list all 11

2.1.6 login-access-list privilege-limit 11

2.1.7 timeout 12

2.1.8 http timeout 13

2.2 Login control and management monitoring and debugging commands 14

2.2.1 show login-access-list 14

2.2.2 show timeout 15

2.2.3 show http 15

Chapter 3 system login 17

3.1 user management 17

3.1.1 username username privilege privilege-value password 17

3.1.2 username change-password 18

3.1.3 username failmax 18

3.1.4 username silent-time 19

3.1.5 username online-max 20

3.1.6 username terminal 20

3.1.7 stop 21
3.2 User Management Monitoring and Debugging Commands 22
3.2.1 show username 22
3.2.2 show username silent 23
3.3 ssh configuration command 25
3.3.1 ssh 25
3.3.2 ssh port 25
3.3.3 crypto key generate 26
3.3.4 crypto key zeroize 27
3.3.5 ssh limit 27
3.3.6 stop vty 28
3.4 ssh monitoring and debugging commands 28
3.4.1 show ssh 28
3.4.2 show ssh limit 30
3.5 telnet configuration command 30
3.5.1 telnet { enable | disable } 30
3.5.2 telnet port 31
3.5.3 telnet limit 32
3.5.4 stop vty 32
3.5.5 telnet ip-address 33
3.5.6 telnet6 ipv6-address 33
3.6 Telent Monitoring and debugging commands 34
3.6.1 show telnet 34
3.6.2 show telnet limit 35
3.7 Web configuration command 35
3.7.1 http 35
3.7.2 http enable ssl 36
3.7.3 load server-certificate 36
3.7.4 load private-key 37
3.7.5 http timeout 38
3.8 Web Monitoring and debugging commands 39
3.8.1 show http 39
3.9 baud-rate configuration command 40
3.9.1 baud-rate 40

Chapter 4 System management 41

4.1 System Management Configuration Commands 41

4.1.1 terminal language 41

4.1.2 hostname 42

4.1.3 cls 42

4.1.4 buildrun mode 43

4.1.5 line width 43

4.1.6 screen-rows per-page 44

4.1.7 clock set 45

4.1.8 clock timezone 45

4.1.9 reboot 46

4.1.10 auto-reboot in 47

4.1.11 auto-reboot at 47

4.2 System Management Monitoring and Debugging Commands 49

4.2.1 show version 49

4.2.2 show system 50

4.2.3 show clock 52

4.2.4 show auto-reboot 52

4.2.5 show memory 53

4.2.6 show screen-rows per-page 54

4.2.7 show line-width 55

4.2.8 show tech-support 55

4.2.9 show cpu-utilization 56

4.2.10 show running-config 57

4.2.11 show startup-config 58

Chapter 5 System log management 59

5.1 System Log Management Configuration Commands 59

5.1.1 logging 59

5.1.2 logging sequence-numbers 59

5.1.3 logging timestamps 60

5.1.4 terminal monitor 61

5.1.5 logging monitor 61

5.1.6 logging monitor { all | monitor-id } { level-id | none | level-list } 62

5.1.7 logging buffered 63
5.1.8 logging buffered { level-id | none | level-list } 64
5.1.9 logging flash 65
5.1.10 logging flash interval 65
5.1.11 logging flash msg-number 66
5.1.12 logging flash { level-id | none | level-list } 67
5.1.13 logging snmp-agent 68
5.1.14 logging snmp-agent { level-id | none | level-list } 69
5.1.15 logging ip-address 69
5.1.16 logging host 70
5.1.17 logging facility 71
5.1.18 logging source 71
5.1.19 logging host { level-id | none | level-list } 72
5.2 System Log Management Monitoring and Debugging Commands 73
5.2.1 show logging 73
5.2.2 show logging filter 75
5.2.3 show logging buffered 76
5.2.4 show logging flash 77
Chapter 6 Software upgrade and configuration file management 79
6.1 Configuration Management 79
6.1.1 copy running-config startup-config 79
6.1.2 copy startup-config running-config 79
6.1.3 clear startup-config [with user-info] 80
6.2 Configure management and debugging commands 80
6.2.1 show running-config 80
6.2.2 show startup-config 81
6.3 file download 82
6.3.1 load application ftp 82
6.3.2 load application tftp 83
6.3.3 load application xmodem 84
6.3.4 load whole-bootrom ftp 84
6.3.5 load whole-bootrom tftp 85
6.3.6 load whole-bootrom xmodem 86

6.3.7 load configuration ftp 86
6.3.8 load configuration tftp 87
6.3.9 load configuration xmodem 88
6.4 File upload 89
6.4.1 upload logging ftp 89
6.4.2 upload logging tftp 89
6.4.3 upload configuration ftp 90
6.4.4 upload configuration tftp 91
Chapter 7 SNTP client 92
7.1 SNTP client configuration command 92
7.1.1 sntp client 92
7.1.2 sntp client mode 92
7.1.3 sntp client authenticate 93
7.1.4 sntp client authentication-key 94
7.1.5 sntp client broadcastdelay 94
7.1.6 sntp client poll-interval 95
7.1.7 sntp client retransmit 96
7.1.8 sntp client retransmit-interval 97
7.1.9 sntp client summer-time dayly 97
7.1.10 sntp client summer-time weekly 98
7.1.11 sntp client valid-server 99
7.1.12 sntp trusted-key 100
7.1.13 sntp server key 101
7.1.14 sntp server 101
7.1.15 sntp server backup 102
7.1.16 sntp client mode anycast key 103
7.2 SNTP client Monitoring and debugging commands 103
7.2.1 show sntp client 103
7.2.2 show sntp client summer-time 105
Chapter 8 Ethernet Port 107
8.1 Ethernet Port Configure Commands 107
8.1.1 interface ethernet 107
8.1.2 interface eth-trunk 107

8.1.3 interface range 108
8.1.4 description 109
8.1.5 speed 109
8.1.6 duplex 111
8.1.7 priority 112
8.1.8 ingress filtering 112
8.1.9 ingress acceptable-frame 113
8.1.10 switchport link-type 114
8.1.11 switchport hybrid 115
8.1.12 switchport pvid 116
8.1.13 shutdown 116
8.1.14 mtu 117
8.1.15 flow-control 118
8.1.16 vct run 119
8.1.17 loopback internal 120
8.1.18 loopback external 120
8.2 Ethernet Port Debug Commands 121
8.2.1 show interface 121
8.2.2 show interface brief 124
8.2.3 clear interface 126
8.2.4 show statistics interface 126
8.2.5 show statistics dynamic 128
8.2.6 show statistics eth-trunk 129
8.2.7 show cpu-statistics 131
8.2.8 clear cpu-statistics 131
8.2.9 show utilization eth-trunk 132
8.2.10 show utilization interface 133
8.2.11 show cpu-utilization 134
8.2.12 show flow-control interface 135
8.2.13 show mtu interface 136
8.2.14 show interface sfp 137
Chapter 9 VLAN Interface 140
9.1 VLAN Interface Configure Commands 140

9.1.1 interface vlan-interface 140
9.1.2 description 140
9.1.3 ip address 141
9.1.4 ip address primary 142
9.1.5 ip address { dhcp | bootp } 143
9.1.6 ip address range 144
9.1.7 ipv6 address { ipv6-address/M | autoconfig } 144
9.1.8 ipv6 address { ipv6-address | auto } link-local 145
9.1.9 ipv6 address ipv6-prefix eui-64 146
9.1.10 ipv6 pathmtu 147
9.1.11 ipv6 nd dad attemps 147
9.1.12 bandwidth 148
9.1.13 shutdown 149
9.2 VLAN Interface Debug Commands 150
9.2.1 show ip interface vlan-interface 150
9.2.2 show ipv6 nd dad attemps 151
9.2.3 show ip dhcp lease 152
9.2.4 show ipv6 interface vlan-interface 152
Chapter 10 Supervlan Interface 155
10.1 Supervlan Interface Commands 155
10.1.1 interface supervlan-interface 155
10.1.2 subvlan 155
10.1.3 description 156
10.1.4 ip address 157
10.1.5 ip address primary 158
10.1.6 ip address { dhcp | bootp } 159
10.1.7 ip address range 159
10.1.8 ipv6 address { ipv6-address/M | autoconfig } 160
10.1.9 ipv6 address { ipv6-address | auto } link-local 161
10.1.10 ipv6 address ipv6-prefix eui-64 162
10.1.11 ipv6 pathmtu 162
10.1.12 ipv6 nd dad attemps 163
10.1.13 bandwidth 164

10.1.14 shutdown 165
10.2 Supervlan Interface Debug Commands 166
10.2.1 show ip interface supervlan-interface 166
10.2.2 show ipv6 nd dad attemps 167
10.2.3 show ip dhcp lease 168
10.2.4 show ipv6 interface supervlan-interface 169
Chapter 11 Loopback Interface 172
11.1 Loopback Interface Configure Commands 172
11.1.1 interface loopback-interface 172
11.1.2 ip address 172
11.1.3 ip address primary 173
11.2 Loopback Interface Debug Commands 174
11.2.1 show ip interface loopback-interface 174
11.2.2 show ipv6 interface loopback-interface 175
Chapter 12 Internal Interface 177
12.1 Internal Interface Configuration Commands 177
12.1.1 interface internal-interface 177
12.1.2 ip address 177
12.2 Management Interface Debug Commands 178
12.2.1 show ip interface internal-interface 178
Chapter 13 LACP 180
13.1 LACP configuration the commands 180
13.1.1 interface eth-trunk 180
13.1.2 link-aggregation mode 180
13.1.3 link-aggregation members 181
13.1.4 link-aggregation eth-trunk 1
13.1.5 lacp mode 183
13.1.6 lacp period 184
13.1.7 lacp port-priority 184
13.1.8 lacp system-priority 185
13.1.9 link-aggregation load-balance 186
13.2 Link aggregation monitoring and debugging the commands 187

13.2.1 show lacp local 187
13.2.2 show lacp neighbor 189
13.2.3 show lacp sys-id 191
13.2.4 debug lacp 192
Chapter 14 Port Isolation 193
14.1 Port isolation configuration the commands 193
14.1.1 port-isolation uplink ethernet 193
14.2 Port isolation monitoring and debugging the commands 194
14.2.1 show port-isolation 194
14.2.2 debug port_isolation 195
Chapter 15 VLAN 196
15.1 VLAN configuration the commands 196
15.1.1 vlan 196
15.1.2 switchport { all | ethernet port-id } 197
15.1.3 description 198
15.1.4 switchport pvid 198
15.1.5 switchport link-type 199
15.1.6 switchport hybrid { untagged | tagged } vlan 200
15.1.7 switchport trunk allowed vlan 201
15.1.8 ingress filtering 202
15.1.9 ingress acceptable-frame 203
15.2 VLAN monitoring and debugging the commands 204
15.2.1 show vlan 204
15.2.2 show vlan brief 205
15.2.3 show vlan brief interface 206
15.2.4 show ingress interface 208
15.3 Mac-VLAN configuration the commands 209
15.3.1 mac-vlan mac-address 209
15.4 Mac-VLAN monitoring and debugging the commands 210
15.4.1 show mac-vlan 210
15.5 IP-subnet-vlan configuration the commands 211
15.5.1 ip-subnet-vlan ipv4 211
15.5.2 ip-subnet-vlan precede 212

15.6 IP-subnet-vlan monitoring and debugging the commands 212

15.6.1 show ip-subnet-vlan 212

15.7 Protocol-VLAN configuration the commands 214

15.7.1 protocol-vlan profile frame-type ether-type 214

15.7.2 protocol-vlan 215

15.7.3 protocol-vlan profile vlan 216

15.8 Protocol-VLAN monitoring and debugging the commands 217

15.8.1 show protocol-vlan profile 217

15.8.2 show protocol-vlan interface 218

15.9 VLAN Swap configuration the commands 219

15.9.1 vlan swap 219

15.10 VLAN-Translate configuration the commands 220

15.10.1 vlan-translate-table { ingress | egress } 220

15.10.2 vlan-translate { ingress | egress } 221

15.11 VLAN-Translate monitoring and debugging the commands 222

15.11.1 show vlan-translate-table 222

15.11.2 show vlan-translate 223

Chapter 16 QinQ 225

16.1 QinQ configuration the commands 225

16.1.1 qinq 225

16.1.2 qinq mode 225

16.1.3 vlan insert 226

16.1.4 vlan pass-through 227

16.1.5 qinq inner-tpid 228

16.1.6 qinq outer-tpid 228

16.2 QinQ monitoring and debugging the commands 229

16.2.1 show qinq 229

Chapter 17 MAC address management 231

17.1 MAC address management configuration the commands 231

17.1.1 mac-address-table age-time 231

17.1.2 mac-address-table max-mac-count 231

17.1.3 mac-address-table permanent 232

17.1.4 mac-address-table blackhole 233

17.1.5 mac-address-table static 234
17.1.6 mac-address-table dynamic 234
17.1.7 mac-address-table learning 235
17.1.8 no mac-address-table 236
17.1.9 no mac-address-table express 237
17.1.10 unknown-discard src-mac 237
17.1.11 local-switch 238
17.2 MAC address management monitoring and debugging the commands 239
17.2.1 show mac-address aging-time 239
17.2.2 show mac-address-table 239
17.2.3 show mac-address-table mac-address 241
17.2.4 show mac-address-table vlan 242
17.2.5 show mac-address-table learning 243
17.2.6 show mac-address-table max-mac-count interface 244
17.2.7 show unknown-discard src-mac 245
17.2.8 show local-switch 246
Chapter 18 Spanning tree protocol 248
18.1 STP/RSTP configuration the commands 248
18.1.1 stp 248
18.1.2 stp mode 249
18.1.3 stp priority 250
18.1.4 stp port-priority 250
18.1.5 stp forward-time 251
18.1.6 stp hello-time 252
18.1.7 stp max-age 253
18.1.8 stp portfast 254
18.1.9 stp link-type 255
18.1.10 stp bpdu-filter 256
18.1.11 stp bpdu-guard 257
18.1.12 stp transit-limit 258
18.1.13 stp loop-guard 258
18.1.14 stp root-guard 259
18.1.15 stp root-guard action 260

18.1.16 stp pathcost-standard 260
18.1.17 stp tc-protection 261
18.1.18 stp tc-protection interval 262
18.1.19 stp tc-protection threshold 263
18.1.20 stp time-factor 263
18.1.21 stp cost 264
18.1.22 stp mcheck 265
18.1.23 stp tcn-restricted 265
18.1.24 clear stp interface 266
18.2 STP/RSTPmonitoring and debugging the commands 267
18.2.1 show stp interface brief 267
18.2.2 show stp interface 269
18.3 MSTP configuration the commands 272
18.3.1 stp 272
18.3.2 stp mode 273
18.3.3 clear stp interface 274
18.3.4 mstp hello-time 275
18.3.5 mstp forward-time 276
18.3.6 mstp max-age 277
18.3.7 mstp time-factor 278
18.3.8 mstp max-hops 279
18.3.9 mstp instance vlan 279
18.3.10 mstp instance priority 280
18.3.11 mstp instance port-priority 281
18.3.12 mstp instance cost 282
18.3.13 mstp external cost 283
18.3.14 mstp revision 283
18.3.15 mstp region-name 284
18.3.16 mstp config-digest-snooping 285
18.3.17 mstp enable instance 285
18.3.18 mstp disable instance 286
18.3.19 mstp portfast 287
18.3.20 mstp link-type 287
18.3.21 mstp bpdu-filter 288

18.3.22 mstp bpdu-guard 289
18.3.23 mstp loop-guard 290
18.3.24 mstp root-guard 291
18.3.25 mstp root-guard action 292
18.3.26 mstp flap-guard 293
18.3.27 mstp flap-guard max-flaps 293
18.3.28 mstp flap-guard recovery-time 294
18.3.29 mstp tc-protection 295
18.3.30 mstp tc-protection interval 296
18.3.31 mstp tc-protection threshold 296
18.3.32 mstp mcheck 297
18.4 MSTP monitoring and debugging the commands 298
18.4.1 show mstp instance brief 298
18.4.2 show mstp instance interface 300
18.4.3 show mstp config-id 302
18.4.4 show mstp disabled-instance 304
Chapter 19 Loopback-detection 306
19.1 loopback-detection configuration the commands 306
19.1.1 loopback-detection 306
19.1.2 loopback-detection interface 307
19.1.3 loopback-detection action 307
19.1.4 loopback-detection interval-time 308
19.2 loopback-detection monitoring and debugging the commands 309
19.2.1 show loopback-detection 309
Chapter 20 ARP 311
20.1 ARP Configuration Commands 311
20.1.1 arp ip-address mac-address 311
20.1.2 arp aging-time 312
20.1.3 arp bind dynamic 312
20.1.4 no arp 313
20.2 ARP Monitoring and Debug Commands 314
20.2.1 show arp 314
20.2.2 show arp { all | dynamic | static } 315

20.2.3 show arp aging-time 317
20.2.4 debug arp 317
Chapter 21 ARP Proxy 319
21.1 ARP Proxy Configuration Commands 319
21.1.1 arp-proxy 319
21.1.2 local-arp-proxy 319
21.2 ARP Proxy Monitoring and Debug Commands 320
21.2.1 show arp-proxy 320
21.2.2 show local-arp-proxy 321
Chapter 22 NDP 323
22.1 NDP Configuration Commands 323
22.1.1 ipv6 nd ns reachable-time 323
22.1.2 ipv6 nd ns retrans-time 323
22.1.3 ipv6 neighbors max-learning-num 324
22.1.4 ipv6 neighbor ipv6-address mac-address 325
22.1.5 no ipv6 neighbor 326
22.2 NDP Monitoring and Debug Commands 326
22.2.1 show ipv6 neighbors 326
22.2.2 show ipv6 neighbors { all | dynamic | static } 328
22.2.3 show ipv6 neighbors max-learning-num 330
22.2.4 show ipv6 nd reachable-time 331
22.2.5 show ipv6 nd ns retrans-time 332
Chapter 23 DHCP server 334
23.1 DHCP Server Configuration Commands 334
23.1.1 dhcp-server 334
23.1.2 dhcp-server server-id 334
23.1.3 dhcp-server ip-pool 335
23.1.4 gateway 336
23.1.5 section 337
23.1.6 lease 338
23.1.7 dns-list 338
23.1.8 domain-name 339

23.1.9 nbns-list 340
23.1.10 forbidden-ip 341
23.1.11 router 341
23.1.12 option 342
23.1.13 dhcp-client bind 343
23.1.14 dhcp-client bind ip-address mac-address vlan-id 344
23.1.15 dhcp-client unbind-assign 344
23.1.16 unbind-client 345
23.2 DHCP Server Monitoring and Debug Commands 346
23.2.1 show dhcp-server 346
23.2.2 show dhcp-server clients 347
23.2.3 show dhcp-server interface 349
23.2.4 show dhcp-server ip-pool 350
23.2.5 show dhcp-client bind 353
23.2.6 debug dhcp 355
Chapter 24 DHCP relay 356
24.1 DHCP Relay Configuration Commands 356
24.1.1 dhcp-relay 356
24.1.2 dhcp-relay hide server-ip 356
24.1.3 dhcp-relay max-hops 357
24.2 DHCP Relay Monitoring and Debug Commands 358
24.2.1 show dhcp-relay 358
24.2.2 debug dhcp 359
Chapter 25 DHCP option60 361
25.1 DHCP Option60 Configuration Commands 361
25.1.1 dhcp-option60 { equals | start-with } { ascii | hex } 361
25.2 DHCP Option60 Monitoring and Debug Commands 362
25.2.1 show dhcp-option60 362
Chapter 26 Routing Fundamentals 364
26.1 Routing foundation Configuring commands 364
26.1.1 router id 364
26.1.2 ip dlf cpu 364

26.1.3 ip host-dlf cpu 365
26.2 Routing foundation monitoring command 366
26.2.1 show router id 366
26.2.2 show ip route 367
26.2.3 show ip fdb 368
26.2.4 show ip lpm 369
26.2.5 show ip dlf cpu 371
26.2.6 show ip host-dlf cpu 371
Chapter 27 IPv6 Routing foundation 373
27.1 IPv6 Routing base configuration command 373
27.1.1 ipv6 forwarding 373
27.2 IPv6 routing foundation monitoring and debugging command 373
27.2.1 show ipv6 route 373
27.2.2 show ipv6 fdb 375
27.2.3 show ipv6 lpm 376
Chapter 28 Static routing 378
28.1 Static routing configuration command 378
28.1.1 ip route 378
28.2 Static routing monitoring and debugging command 379
28.2.1 show ip route 379
Chapter 29 IPv6 Static routing 381
29.1 IPv6 Static routing configuration command 381
29.1.1 ipv6 route 381
29.2 IPv6 Static routing monitoring and debugging command 382
29.2.1 show ipv6 route 382
Chapter 30 RIP 384
30.1 RIP Configuring commands 384
30.1.1 router rip 384
30.1.2 network 384
30.1.3 ip rip authentication 385
30.1.4 aggregate-address 386
30.1.5 default-information originate 387

30.1.6 default-metric 388
30.1.7 distance 388
30.1.8 distribute-list 389
30.1.9 offset-list 391
30.1.10 redistribute 392
30.1.11 route 393
30.1.12 timers basic 393
30.1.13 passive-interface 394
30.1.14 ip rip receive version 395
30.1.15 ip rip send version 396
30.1.16 version 397
30.1.17 ip rip split-horizon 398
30.1.18 ip rip split-horizon poisoned-reverse 399
30.1.19 key chain 400
30.1.20 key 401
30.1.21 key-string 401
30.1.22 accept-lifetime 402
30.1.23 send-lifetime 403
30.1.24 route-map in 404
30.1.25 route-map out 405
30.2 RIP Monitoring and debugging commands 406
30.2.1 show rip route-table 406
30.2.2 show ip rip interface 409
30.2.3 show ip rip status 411
30.2.4 debug rip 413
30.2.5 debug ip rip 414
Chapter 31 RIPng 416
31.1 RIPng Configuring commands 416
31.1.1 router ripng 416
31.1.2 ipv6 router ripng 416
31.1.3 aggregate-address 417
31.1.4 default-information originate 418
31.1.5 default-metric 419

31.1.6 distribute-list 419
31.1.7 ipv6 ripng split-horizon 421
31.1.8 ipv6 ripng split-horizon poisoned-reverse 421
31.1.9 offset-list 422
31.1.10 redistribute 423
31.1.11 timers basic 424
31.1.12 route-map in 425
31.1.13 route-map out 426
31.2 The RIPng monitoring and debugging command 427
31.2.1 show ripng route-table 427
31.2.2 show ipv6 ripng status 429
31.2.3 show ipv6 ripng interface 432
31.2.4 debug ripng 433
31.2.5 debug ipv6 ripng 434
Chapter 32 OSPF 436
32.1 OSPF Configuring commands 436
32.1.1 router ospf 436
32.1.2 ospf router-id 436
32.1.3 network area 437
32.1.4 area authentication 438
32.1.5 ip ospf authentication 439
32.1.6 ip ospf authentication-key 440
32.1.7 ip ospf message-digest-key 441
32.1.8 area default-cost 442
32.1.9 default-information originate 443
32.1.10 default-metric 444
32.1.11 distance 445
32.1.12 ip ospf bfd 446
32.1.13 area range 447
32.1.14 distribute-list 448
32.1.15 area shortcut 449
32.1.16 area nssa 450
32.1.17 area stub 451

32.1.18 area virtual-link 452
32.1.19 area filter-list 454
32.1.20 auto-cost reference-bandwidth 455
32.1.21 bandwidth 456
32.1.22 capability opaque 456
32.1.23 ip ospf cost 457
32.1.24 ip ospf dead-interval 458
32.1.25 ip ospf hello-interval 459
32.1.26 ip ospf mtu-ignore 460
32.1.27 ip ospf network 461
32.1.28 ip ospf priority 462
32.1.29 ip ospf retransmit-interval 463
32.1.30 ip ospf transmit-delay 464
32.1.31 log-adjacency-changes 465
32.1.32 neighbor 466
32.1.33 ospf abr-type 466
32.1.34 ospf rfc1583 compatibility 467
32.1.35 passive-interface 468
32.1.36 redistribute 469
32.1.37 refresh timer 470
32.1.38 timers throttle spf 471
32.2 OSPF Monitoring and debugging commands 472
32.2.1 show ip ospf neighbor 472
32.2.2 show ospf route-table 474
32.2.3 show ip ospf 476
32.2.4 show ip ospf border-routers 479
32.2.5 show ip ospf database 481
32.2.6 show ip ospf interface 483
32.2.7 show ip ospf virtual-link 486
32.2.8 debug ospf 487
32.2.9 debug ip ospf 488
Chapter 33 Routing policy 491
33.1 Routing policy configuration command 491

33.1.1 ip access-list 491
33.1.2 ip prefix-list 493
33.1.3 ip prefix-list sequence-number 494
33.1.4 ipv6 access-list 495
33.1.5 ipv6 prefix-list 496
33.1.6 ipv6 prefix-list sequence-number 498
33.1.7 route-map 498
33.1.8 match interface 500
33.1.9 match ip address 501
33.1.10 match ip next-hop 502
33.1.11 match ip route-source 502
33.1.12 match metric 503
33.1.13 match tag 504
33.1.14 match as-path 505
33.1.15 match origin 506
33.1.16 match probability 507
33.1.17 set ip next-hop 508
33.1.18 set metric 508
33.1.19 set metric-type 509
33.1.20 set tag 510
33.1.21 set local-preference 511
33.1.22 set origin 512
33.1.23 set weight 513
33.1.24 call 514
33.1.25 continue 515
33.1.26 on-match 516
33.1.27 route-map in 516
33.1.28 route-map out 517
33.2 Routing policy monitoring and debugging command 518
33.2.1 show route-map 518
33.2.2 clear ip prefix-list 520
33.2.3 clear ipv6 prefix-list 520
33.2.4 show ip access-list 521
33.2.5 show ip prefix-list 522

33.2.6 show ipv6 access-list 524
33.2.7 s show ipv6 prefix-list 525

Chapter 34 L2 Multicast Basic 527

34.1 L2 Multicast basic config command 527
34.1.1 unknown-discard multicast vlan 527
34.1.2 multicast mac-address vlan 527
34.1.3 multicast mac-address vlan interface 528
34.2 L2 Multicast Basic Monitor and Debug 529
34.2.1 show unknown-discard vlan 529
34.2.2 show multicast 530
34.2.3 debug multicast 531

Chapter 35 IGMP-snooping 533

35.1 IGMP-snooping config command 533
35.1.1 igmp-snooping 533
35.1.2 igmp-snooping enable-vlan 533
35.1.3 igmp-snooping version 534
35.1.4 igmp-snooping host-aging-time 535
35.1.5 igmp-snooping max-response-time 535
35.1.6 igmp-snooping robust-count 536
35.1.7 igmp-snooping last-member-query-interval 537
35.1.8 igmp-snooping fast-leave 537
35.1.9 igmp-snooping group-limit 538
35.1.10 igmp-snooping overflow-replace 539
35.1.11 igmp-snooping drop 540
35.1.12 igmp-snooping multicast-vlan 541
35.1.13 igmp-snooping static-group 541
35.1.14 igmp-snooping static-group proxy 542
35.1.15 igmp-snooping source-learning 543
35.1.16 igmp-snooping querier 544
35.1.17 igmp-snooping querier-vlan 544
35.1.18 igmp-snooping querier-elect 545
35.1.19 igmp-snooping query-interval 546
35.1.20 igmp-snooping query-source 546

35.1.21 igmp-snooping proxy 547
35.1.22 igmp-snooping query-proxy 548
35.1.23 igmp-snooping route-port 549
35.1.24 igmp-snooping router-aging-time 549
35.1.25 igmp-snooping route-port forward 550
35.1.26 igmp-snooping preview 551
35.1.27 igmp-snooping preview group-ip 552
35.1.28 igmp-snooping preview time-once 552
35.1.29 igmp-snooping preview time-interval 553
35.1.30 igmp-snooping preview permit-times 554
35.1.31 igmp-snooping preview time-reset 554
35.1.32 igmp-snooping profile 555
35.1.33 profile limit 556
35.1.34 ip range 556
35.1.35 mac range 557
35.1.36 description 558
35.1.37 igmp-snooping profile refer 559
35.1.38 igmp-snooping { permit | deny } group all 559
35.1.39 igmp-snooping { permit | deny } { group | group-range } 560
35.2 IGMP-snooping monitoring and debugging commands 561
35.2.1 clear igmp-snooping statistics 561
35.2.2 show igmp-snooping 561
35.2.3 show igmp-snooping mcast-table 565
35.2.4 show igmp-snooping static-table 566
35.2.5 show igmp-snooping fib-table 568
35.2.6 show igmp-snooping router-dynamic 569
35.2.7 show igmp-snooping router-static 570
35.2.8 show igmp-snooping preview 571
35.2.9 show igmp-snooping preview status 572
35.2.10 show igmp-snooping profile 573
35.2.11 show igmp-snooping profile ethernet 575
35.2.12 show igmp-snooping profile vlan 576
35.2.13 show igmp-snooping statistics 578
35.2.14 debug igmp_snooping 581

Chapter 36 IPv4 Multicast Basics 582

36.1 IPv4 multicast basic configuration commands 582

36.1.1 ip multicast-routing 582

36.1.2 mroute igmp 582

36.1.3 mroute pim 583

Chapter 37 IPv6 Multicast Basics 584

37.1 IPv6 Multicast Basic Configuration Commands 584

37.1.1 multicast mac-address vlan 584

37.1.2 multicast mac-address vlan interface 585

37.2 IPv6 Multicast Basic Monitoring and Debugging Commands 585

37.2.1 show multicast mld-snooping 585

37.2.2 debug multicast 587

Chapter 38 CoS 588

38.1 CoS configure command 588

38.1.1 queue-scheduler group-id strict-priority 588

38.1.2 queue-scheduler group-id wfq 588

38.1.3 queue-scheduler group-id sp-wfq 589

38.1.4 queue-scheduler group-id wrr 590

38.1.5 queue-scheduler group-id sp-wrr 591

38.1.6 queue-scheduler cos-map group-id priority queue 592

38.1.7 queue-scheduler cos-map group-id 592

38.1.8 queue-scheduler dscp-map 593

38.1.9 queue-scheduler dscp-map group-id dscp priority 594

38.1.10 queue-scheduler group-id 595

38.1.11 queue-scheduler dscp-map group-id 595

38.2 CoS Monitoring and debugging command 596

38.2.1 show queue-scheduler 596

38.2.2 show queue-scheduler cos-map 597

38.2.3 show queue-scheduler dscp-map 598

38.2.4 show queue-scheduler port-map 600

Chapter 39 ACL 1

39.1 ACL configure command 602

39.1.1 access-list acl-id match-order 602
39.1.2 access-list step 602
39.1.3 access-list mac-acl-id 603
39.1.4 access-list ip-acl-id 604
39.1.5 access-list hybrid-acl-id 607
39.1.6 access-list { mac-acl | ip-acl | hybrid-acl } acl-id 609
39.1.7 subitem-id { permit | deny } (MAC-ACL) 610
39.1.8 subitem-id { permit | deny } (IP-ACL) 612
39.1.9 subitem-id { permit | deny } (Hybrid-ACL) 614
39.1.10 access-group 616
39.1.11 time-range 617
39.1.12 absolute 618
39.1.13 periodic 619
39.2 ACL Monitoring and debugging command 620
39.2.1 show time-range 620
39.2.2 show access-list config 621
39.2.3 show access-list runtime 622
Chapter 40 QACL 623
40.1 QACL configure command 623
40.1.1 traffic priority 623
40.1.2 traffic insert-vlan 624
40.1.3 traffic rewrite-vlan 625
40.1.4 traffic redirect 626
40.1.5 traffic statistic 627
40.1.6 traffic mirror 628
40.1.7 traffic rate-limit 629
40.2 QACL Monitoring and debugging command 630
40.2.1 show traffic 630
Chapter 41 Two-speed three-color 632
41.1 Two-speed three-color configuration command 632
41.1.1 two-rate-policer mode 632
41.1.2 two-rate-policer set-pre-color 632
41.1.3 two-rate-policer policer-id 633

41.1.4 traffic rate-limit acl-id two-rate-policer 635
41.2 Two-speed three-color monitoring and debugging command 635
41.2.1 show two-rate-policer [policer-id] 635
41.2.2 show two-rate-policer 637
Chapter 42 bandwidth control 640
42.1 Bandwidth control configuration command 640
42.1.1 bandwidth ingress 640
42.1.2 bandwidth egress 641
42.1.3 bandwidth queue 642
42.2 Bandwidth control, monitoring and debugging command 642
42.2.1 show bandwidth interface 642
42.2.2 show bandwidth queue interface 643
Chapter 43 Storm-control 645
43.1 Storm-control configuration commands 645
43.1.1 storm-control action 645
43.1.2 storm-control { broadcast | multicast | unicast } 646
43.2 Storm-control monitoring commands 647
43.2.1 show storm-control interface 647
Chapter 44 ARP anti-spoofing 649
44.1 ARP anti-spoofing configuration commands 649
44.1.1 arp anti-spoofing 649
44.1.2 arp anti-spoofing action 649
44.1.3 arp anti-spoofing bind 650
44.1.4 arp anti-spoofing gateway-disguiser 651
44.1.5 arp anti-spoofing source-mac-check 652
44.1.6 arp anti-attack trust 652
44.2 ARP anti-spoofing monitoring commands 653
44.2.1 show arp anti-spoofing 653
44.2.2 show arp anti-spoofing bind 654
44.2.3 show arp anti-attack 656
Chapter 45 ARP anti-flood 658
45.1 ARP anti-flood configuration commands 658

45.1.1 arp anti-flood 658
45.1.2 arp anti-flood action 658
45.1.3 arp anti-flood rate-limit 659
45.1.4 arp anti-flood recover-time 660
45.1.5 arp anti-flood recover 661
45.1.6 arp anti-flood bind blackhole 661
45.2 ARP anti-flood monitoring commands 662
45.2.1 show arp anti-flood 662
45.2.2 show arp anti-flood rate-limit 664
Chapter 46 Attack detection 666
46.1 Attack detection configuration commands 666
46.1.1 cpu-car 666
46.1.2 alarm cpu 666
46.1.3 alarm cpu threshold busy 667
46.1.4 alarm all-packets 668
46.1.5 alarm all-packets threshold 668
46.1.6 system trap { enable | disable } 669
46.1.7 system trap period 670
46.1.8 port-car 671
46.1.9 port-car rate 671
46.1.10 bpdu-discard 672
46.1.11 anti-dos packets class 673
46.1.12 dhcp anti-attack 674
46.1.13 dhcp anti-attack action 675
46.1.14 dhcp anti-attack bind blackhole 675
46.1.15 dhcp anti-attack threshold 676
46.1.16 dhcp anti-attack recover-time 677
46.1.17 dhcp anti-attack recover 677
46.1.18 dhcp anti-attack trust 678
46.1.19 cpu-attack threshold 679
46.1.20 cpu-attack protect 679
46.1.21 cpu-ratelimit 680
46.1.22 ip dlf cpu 681

46.1.23 ip host-dlf cpu 682
46.2 Attack detection monitoring commands 683
46.2.1 show cpu-car 683
46.2.2 show cpu-statistics 683
46.2.3 clear cpu-statistics 685
46.2.4 show cpu-classification 686
46.2.5 clear cpu-classification 687
46.2.6 show cpu-utilization 688
46.2.7 show port-car 688
46.2.8 show anti-dos 690
46.2.9 show bpdu-discard 690
46.2.10 show dhcp anti-attack 691
46.2.11 show dhcp anti-attack interface 692
46.2.12 show alarm cpu 693
46.2.13 show alarm all-packets 694
46.2.14 show alarm all-packets interface 695
46.2.15 show ip dlf cpu 696
46.2.16 show ip host-dlf cpu 697
46.2.17 show cpu-attack interface 697

Chapter 47 IP-source-guard 700

47.1 ip-source-guard configuration command 700
47.1.1 ip source 700
47.1.2 ip source bind 701
47.1.3 ip source vlan 702
47.1.4 ip source permit-igmp 702
47.2 ip-source-guard monitor command 703
47.2.1 show ip source bind 703
47.2.2 show ip source vlan 704
47.2.3 show ip source permit-igmp 705
47.2.4 show ip source 705

Chapter 48 DHCP-snooping 707

48.1 dhcp-snooping configuration command 707
48.1.1 dhcp-snooping 707

48.1.2 dhcp-snooping trust 707
48.1.3 dhcp-snooping fast-remove 708
48.1.4 dhcp-snooping max-learn-num 709
48.1.5 dhcp-snooping dhcp-server 710
48.2 dhcp-snooping monitor command 710
48.2.1 show dhcp-snooping interface 710
48.2.2 show dhcp-snooping vlan 712
48.2.3 show dhcp-snooping clients 713
48.2.4 clear dhcp-snooping 714
48.2.5 debug dhcpsnooping 715
Chapter 49 DHCP option82 717
49.1 dhcp option82 configuration command 717
49.1.1 dhcp-option82 717
49.1.2 dhcp-option82 format 718
49.1.3 dhcp-option82 format verbose node-identifier 718
49.1.4 dhcp-option82 information format 719
49.1.5 dhcp-option82 circuit-id 720
49.1.6 dhcp-option82 remote-id 721
49.1.7 dhcp-option82 strategy 721
49.1.8 dhcp-option82 device-id 722
49.2 dhcp option82 monitor command 723
49.2.1 show dhcp-option82 interface 723
49.2.2 show dhcp-option82 vlan 725
Chapter 50 DLF control 727
50.1 DLF control configuration commands 727
50.1.1 unknown-discard unicast 727
50.1.2 unknown-discard multicast vlan 727
50.2 Monitoring commands for DLF control 728
50.2.1 show unknown-discard ethernet 728
50.2.2 show unknown-discard vlan 729
Chapter 51 SLF control 731
51.1 SLF control configuration command 731

51.1.1 unknown-discard src-mac 731
51.2 Monitoring commands for SLF control 731
51.2.1 show unknown-discard src-mac 731
Chapter 52 ErrorDisable 733
52.1 ErrorDisable configuration command 733
52.1.1 errdisable detect cause 733
52.1.2 errdisable recovery cause 734
52.1.3 errdisable recovery interval 735
52.2 ErrorDisable manages monitoring and debugging commands 735
52.2.1 show errdisable 735
Chapter 53 ERPS 738
53.1 ERPS configuration command 738
53.1.1 erps 738
53.1.2 erps instance 738
53.1.3 control-vlan 739
53.1.4 guard-timer 740
53.1.5 mel 741
53.1.6 port0 742
53.1.7 port1 743
53.1.8 protected-instance 744
53.1.9 ring 745
53.1.10 ring level 746
53.1.11 ring enable 747
53.1.12 work-mode 747
53.1.13 wtr-timer 748
53.2 ERPS monitoring and debugging Command 749
53.2.1 show erps 749
53.2.2 show erps statistics 752
53.2.3 show erps instance 753
53.2.4 show erps control-vlan 757
53.2.5 clear erps statistics 759
53.2.6 debug erps 759

Chapter 54 VRRP 761

54.1 VRRP Configuration Command 761

54.1.1 vrrp vrid virtual-ip 761

54.1.2 vrrp vrid advertise-interval 762

54.1.3 vrrp vrid preempt-mode 763

54.1.4 vrrp vrid preempt-mode delay 764

54.1.5 vrrp vrid priority 764

54.1.6 vrrp vrid track 765

54.2 VRRP Monitoring and Commissioning command 766

54.2.1 show vrrp status 766

54.2.2 show vrrp statistics 768

54.2.3 debug vrrp 771

Chapter 55 Network Testing & Troubleshooting 772

55.1 Network testing and troubleshooting commands 772

55.1.1 ping 772

55.1.2 ping6 773

55.1.3 tracert 774

55.1.4 tracert6 775

Chapter 56 SNMP 777

56.1 SNMP configuration commands 777

56.1.1 snmp-server { enable | disable } 777

56.1.2 snmp-server contact 777

56.1.3 snmp-server location 778

56.1.4 snmp-server name 779

56.1.5 snmp-server community 780

56.1.6 snmp-server view 780

56.1.7 snmp-server group 781

56.1.8 snmp-server user 782

56.1.9 snmp-server user remote 784

56.1.10 snmp-server enable { traps | informs } 786

56.1.11 snmp-server host 786

56.1.12 snmp-server trap-source 788

56.1.13 snmp-server engineid 788
56.1.14 snmp-server max-packet-length 789
56.2 SNMP Monitoring Command 790
56.2.1 show snmp-server community 790
56.2.2 show snmp-server contact 791
56.2.3 show snmp-server engineid 792
56.2.4 show snmp-server group 793
56.2.5 show snmp-server host 794
56.2.6 show snmp-server location 795
56.2.7 show snmp-server max-packet-length 796
56.2.8 show snmp-server name 797
56.2.9 show snmp-server notify 798
56.2.10 show snmp-server user 799
56.2.11 show snmp-server view 800
56.2.12 debug snmp 801
Chapter 57 RMON 803
57.1 RMON Configuration Command 803
57.1.1 rmon event 803
57.1.2 rmon alarm 804
57.1.3 rmon statistics 805
57.1.4 rmon history 806
57.2 RMON Monitoring Command 807
57.2.1 show rmon alarm 807
57.2.2 show rmon event 808
57.2.3 show rmon eventlog 809
57.2.4 show rmon history 810
57.2.5 show rmon statistics 812
57.2.6 debug rmon 814
Chapter 58 Port Mirror 816
58.1 Port mirror configuration commands 816
58.1.1 mirror group id source-interface 816
58.1.2 mirror group id destination-interface 817
58.1.3 no mirror group all 817

58.2 Remote mirroring configuration commands 818

58.2.1 mirror group id source-interface 818

58.2.2 mirror group id destination-interface ethernet port-id rspan local 819

58.2.3 mirror group id destination-interface ethernet port-id rspan middle 820

58.2.4 mirror group id destination-interface ethernet port-id rspan target 821

58.2.5 no mirror group all 822

58.3 Mirror monitor commands 823

58.3.1 show mirror group 823

58.3.2 debug mirror 824

Chapter 59 LLDP 825

59.1 LLDP Configure Cmomands 825

59.1.1 lldp 825

59.1.2 lldp hello-time 825

59.1.3 lldp hold-time 826

59.1.4 lldp trap 827

59.1.5 lldp { rx | tx | rxtx } 827

59.1.6 lldp management-address 828

59.2 LLDP Debug Commands 829

59.2.1 show lldp 829

59.2.2 debug lldp 830

Chapter 1 Fundamentals of system operation

1.1 Basic configuration commands for system operation

1.1.1 enable

【Command】

enable

【Config-mode】

Execute user mode

【Parameter】

None

【Description】

enable command used to enter privileged user mode from execution user mode.

【Example】

#Enter privileged user mode from execution user mode.

Switch>enable

Switch#

1.1.2 end

【Command】

end

【Config-mode】

Other modes besides executing user mode and privileged user mode.

【Parameter】

None

【Description】

end command used to return to privileged user mode.

【Example】

#From port configuration mode to privileged user mode.

Switch(config)#interface ethernet 0/0/5

Switch(config-if-ethernet-0/0/5)#end

Switch#

1.1.3 configure terminal

【Command】

configure terminal

【Config-mode】

privileged user mode

【Parameter】

None

【Description】

configure terminal command used to privileged user mode enters global configuration mode.

【Example】

#Privileged user mode enters global configuration mode.

Switch#configure terminal

Switch(config)#

1.1.4 exit

【Command】

exit

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

exit command used to return the previous mode of the current configuration mode,can be executed in any mode.If the current mode is executing user mode,execute **exit** Command to log out.

【Example】

#From privileged user mode to executive user mode,then log out.

Switch#exit

Switch>exit

Switch>

Username(1-64 chars):

1.1.5 quit

【Command】

quit

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

quit command used to log out.

【Example】

#Log out of port configuration mode.

Switch(config-if-ethernet-0/0/1)#quit

Username(1-64 chars):

1.1.6 help

【Command】

help

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

help command used to obtain the basic help information about the operation command line,can be executed in any configuration mode,execution displays differently in different modes.

【Example】

#Get help information in privileged user mode

Switch#help

System mode commands:

clear clear information record

cls clear screen

help description of the interactive help

ping Ping command

ping6 Ping command for IPv6

quit disconnect from Switch and quit

show show system information

tracert tracert command

Privilege EXEC mode commands:

buildrun mode to build running-config

clear clear config file in flash

clock clock information

configure Switch to global configure mode

copy copy config file

crypto config cryptography policy

exit return to frontal mode

line Set line information

load download application or configuration

no restore to default value or delete

reboot perform reboot operation

screen-rows Screen rows information in page handling

show show system information

stop Stop running

telnet IPv4 telnet

telnet6 IPv6 telnet

terminal change language mode

timeout config system idle timeout information, default is 20 minutes

upload group commands of upload upgrade program

1.1.7 Shortcut key

The device supports the following command line shortcut keys.

shortcut key	description
Up cursor key（↑）	If there is an earlier command, the previous command is displayed. If the command is the earliest in the history, pressing this key does not change the screen.
Ctrl+P	The function is the same as the up cursor key（↑）.
Down cursor key（↓）	If there are more recent history commands, the next command is displayed. If the command is the latest one in the history, pressing this key does not change the screen.
Ctrl+N	The function is the same as the down cursor key（↓）.
Left cursor key（←）	The cursor moves one character to the left. If the cursor is at the beginning of a command, pressing this key does not change the screen.
Ctrl+B	The function is the same as the left cursor key（←）.
Right cursor key（→）	Move the cursor one character to the right. If the cursor is at the end of the command, pressing this key does not change the screen.
Ctrl+F	The function is the same as the right cursor key（→）.
Tab	● Enter the keyword and press Tab; ● If the matched keyword is unique, all command keywords are automatically completed, and the cursor is one space away from the end of the word; ● If the matched keyword is not unique, the system automatically completes the keyword. For example, if you enter dh globally and press tab, the system automatically completes dhcp; ● If you enter an incorrect keyword, no action is taken after you press Tab.
Ctrl+A	Move the cursor to the beginning of the line.

shortcut key	description
Ctrl+C	To interrupt some running operations,Such as **ping** etc.
Ctrl+D or Delete	Delete the character where the cursor is located.
Ctrl+H or Backspace	Deletes the character before the cursor. If the cursor is at the beginning of a command, pressing this key does not change anything on the screen.
Ctrl+E	Move the cursor to the end of the line.
Ctrl+I	Move the cursor to the end of the line.
Ctrl+K	Delete all characters after the cursor position (including the cursor position).
Ctrl+U	Delete all characters before the cursor position (excluding the cursor position).
Ctrl+J	Line feed
Ctrl+M	Line feed
Ctrl+Z	Back to privileged user mode from other mode (excluding executive user mode).
Enter	When the command line information printed in the terminal column exceeds the screen, the information in the next line is displayed.
Q	When the command line information printed in the terminal column exceeds the screen,exit display.

Chapter 2 Login control and management

2.1 Login control and management configuration commands

2.1.1 login-access-list telnet

【Command】

login-access-list telnet *ip-address wildcard*

no login-access-list telnet { all | *ip-address wildcard }*

【Config-mode】

Global configuration mode

【Parameter】

ip-address: IP address, dotted decimal, the format is: x.x.x.x.

wildcard: network wildcard-mask, 0.0.0.0-255.255.255.255.

【Description】

login-access-list telnet command used to configure the network address that allows you to access the system through telnet.

no login-access-list telnet command used to delete the network address that allows telnet to access the system.

By default, all users are allowed to access the system through telnet,If only specified network addresses are allowed, delete all network addresses first.

【Example】

#Only users on the 192.168.1.0/24 network are allowed to access the system through telnet.

Switch(config)#no login-access-list telnet all

Switch(config)#login-access-list telnet 192.168.1.16 0.0.0.255

2.1.2 login-access-list ssh

【Command】

login-access-list ssh *ip-address wildcard*

no login-access-list ssh { all | *ip-address wildcard }*

【Config-mode】

Global configuration mode

【Parameter】

ip-address: IP address,dotted decimal,the format is:x.x.x.x.

Wildcard:network wildcard-mask, 0.0.0.0-255.255.255.255.

【Description】

login-access-list ssh command is used to configure the network address that allows you to access the system through ssh.

no login-access-list ssh command is used to delete the network address that allows ssh to access the system.

By default, all users are allowed to access the system through ssh. If only specified network address are allowed, delete all network address first.

【Example】

#Only users on the 192.168.1.0/24 network are allowed to access the system through ssh.

Switch(config)#no login-access-list ssh all

Switch(config)#login-access-list ssh 192.168.1.16 0.0.0.255

2.1.3 login-access-list snmp

【Command】

login-access-list snmp *ip-address wildcard*

no login-access-list snmp { all | *ip-address wildcard* }

【Config-mode】

Global configuration mode

【Parameter】

ip-address: IP address,otted decimal, the format is:x.x.x.x.

Wildcard: network wildcard-mask, 0.0.0.0-255.255.255.255.

【Description】

login-access-list snmp command is used to configure the network address that allows you to access the system through snmp.

no login-access-list snmp command is used to delete the network address that allows snmp to access the system.

By default, all users are allowed to access the system through snmp. If only specified network address are allowed, delete all network address first.

【Example】

#Only users on the 192.168.1.0/24 network are allowed to access the system through snmp.

Switch(config)#no login-access-list snmp all

Switch(config)#login-access-list snmp 192.168.1.16 0.0.0.255

2.1.4 login-access-list web

【Command】

login-access-list web *ip-address wildcard*

no login-access-list web { all | *ip-address wildcard }*

【Config-mode】

Global configuration mode

【Parameter】

ip-address: IP address, dotted decimal, the format is:x.x.x.x.

Wildcard: network wildcard-mask, 0.0.0.0-255.255.255.255.

【Description】

login-access-list web command is used to configure the network address that allows you to access the system through web.

no login-access-list web command is used to delete the network address that allows web to access the system.

By default, all users are allowed to access the system through the web UI. If only specified network address are allowed, delete all network address first.

【Example】

#Only users on the 192.168.1.0/24 network are allowed to access the system through the web UI.

Switch(config)#no login-access-list web all

Switch(config)#login-access-list web 192.168.1.16 0.0.0.255

2.1.5 no login-access-list all

【Command】

no login-access-list web all

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

no login-access-list all command is used to deny all terminals from accessing the system.

By default, all users are allowed to access the system.

This command is used to configure the following commands:

no login-access-list telnet

no login-access-list ssh

no login-access-list snmp

no login-access-list web

【Example】

#No terminal is allowed to access the system.

Switch(config)#no login-access-list all

2.1.6 login-access-list privilege-limit

【Command】

login-access-list privilege-limit *limit-value*

no login-access-list privilege-limit

【Config-mode】

Global configuration mode

【Parameter】

limit-value: Number of users,the value ranges from 0 to 5, the default value is 5.

【Description】

login-access-list privilege-limit command is used to configure the number of users who log in remotely and enter the privileged user mode at the same time.

no login-access-list privilege-limit Command is used to restore default values.

By default, a maximum of five users are allowed to remotely log in and enter the privileged user mode at the same time.

【Example】

#Configure the number of users allowed to log in remotely at the same time as three users.

Switch(config)#login-access-list privilege-limit 3

2.1.7 timeout

【Command】

timeout [*time-value*]

no timeout

【Config-mode】

Privileged user mode.

【Parameter】

time-value: timeout, the value ranges from 1 to 480 minutes,the default value is 20 minutes.

【Description】

timeout [*time-value*] this command is used to enable the system timeout function and set the system timeout period.

no timeout the command is used to disable the timeout exit function.

If the value is not time-value, the default value is 20 minutes.

【Example】

#Set the system timeout period to 10 minutes.

Switch#timeout 10

The idle time is : 10 minutes!

2.1.8 http timeout

【Command】

http timeout *time-value*

no http timeout

【Config-mode】

Global configuration mode

【Parameter】

time-value: timeout, the value ranges from 60 to 36000 seconds. The default value is 1200 seconds.

【Description】

http timeout *time-value*,the command is used to set the timeout period of the web terminal.

no http timeout the command is used to restore default configuration.

By default, the timeout period of the web terminal is 1200 seconds.

This command applies only to web terminals.

【Example】

#Configuration the web terminal timeout period to 600 seconds.

Switch(config)#http timeout 600

2.2 Login control and management monitoring and debugging commands

2.2.1 show login-access-list

【Command】

show login-access-list

【Config-mode】

Any configuration mode.

【Parameter】

None

【Description】

show login-access-list the command is used to display the IP address restriction.

【Example】

#View the restriction information about login IP address.

Switch(config)#show login-access-list

sno	ipAddress	wildcard bits	terminal
1	0.0.0.0	255.255.255.255	snmp
2	192.168.1.0	0.0.0.255	snmp
3	0.0.0.0	255.255.255.255	web
4	0.0.0.0	255.255.255.255	telnet
5	192.168.1.0	0.0.0.255	telnet
6	0.0.0.0	255.255.255.255	ssh

show login-access-list display field description

Fields	Description

sno	Serial number
ipAddress	IP address allowed for login
wildcard bits	wildcard-mask
terminal	Terminal type

2.2.2 show timeout

【Command】

show timeout

【Config-mode】

Arbitrary configuration mode.

【Parameter】

None.

【Description】

show timeout the command is used to view the system timeout period.

【Example】

#View the system timeout period.

Switch#show timeout

The idle time is : 10 minutes!

2.2.3 show http

【Command】

show http

【Config-mode】

Arbitrary configuration mode.

【Parameter】

None

【Description】

show http command is used to view http configuration information.

【Example】

#View http configuration information.

Switch#show http

Web Server status:

Running:TRUE

Port:80

Timeout:1200(s)

show http display field description

Fields	Description
Running	Enabled state
Port	Transport layer port number
Timeout	Timeout period

Chapter 3 system login

3.1 user management

3.1.1 username username privilege privilege-value password

【Command】

username *username* **privilege** *privi-value* **password { 0 | 7 }** *password-value*

no username *username*

【Config-mode】

Global configuration mode

【Parameter】

Username: user name,string format,maximum length 64.

privilege-value: User level. The value ranges from 0 to 15. 0-1 indicates the normal level and 2-15 indicates the admin level.

0: Indicates that password-value is a plaintext password.

7: Indicates that password-value is a ciphertext password.

password-value: password,string format,maximum length 64.

【Description】

username *username* **privilege** *privilege-value* **password { 0 | 7 }**command is used to create a new user.

no username *username* command is used to delete a specified user.

By default, user admin, password admin, level 15.

If the created user already exists, run this command to change the *privilege* or password.

Configuration does not enter decompile, write directly to flash.

【Example】

#Configure user test: permission level:5,plaintext password.

Switch(config)#username test privilege 5 password 0 test

3.1.2 username change-password

【Command】

username change-password

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

username change-password command used to change a user password.

【Example】

#Change the password of user admin.

Switch(config)#username change-password

Please input your login password:*****

Please input username:admin

Please input user new password:*********

Please input user confirm password:*********

Change user admin password successfully.

Switch(config)#

3.1.3 username failmax

【Command】

username failmax [*user-name*] *failmax-value*

no username failmax [*username*]

【Config-mode】

Global configuration mode

【Parameter】

failmax-value: Maximum number of failures. The value ranges from 3 to 8. The default value is 5.

username: username,the value is a string of up to 64 characters.

【Description】

username failmax command is used to set the number of silent login failures.

no username failmax command is used to restore default settings.

By default, the number of silent login failures is 5.

The configuration of specific users takes precedence over the global configuration.

The silent function is forcibly enabled and cannot be disabled.

【Example】

#The maximum number of silent login failures was set to 4.

Switch(config)#username failmax admin 4

3.1.4 username silent-time

【Command】

username silent-time *time-value*

【Config-mode】

Global configuration mode

【Parameter】

time-value: The value ranges from 2 to 1440 (unit: minute). The default value is 2.

【Description】

username silent-time command is used to set the silent time.

【Example】

#Set the silence time to 10 minutes.

Switch(config)#username silent-time 10

3.1.5 username online-max

【Command】

username online-max *username online-max-num*

no username online-max *username*

【Config-mode】

Global configuration mode

【Parameter】

username: The value is a string of up to 64 characters.

online-max-num: The value ranges from 1 to 100 maximum online users. The default value is N/A.

【Description】

username online-max command is used to set the maximum number of concurrent online users for the same user.

no username online-max the command is used to restore default settings.

By default,**online-max** is not configured.

Command does not enter decompile.

【Example】

#Set the number of concurrent online users of user admin to 8.

Switch(config)#username online-max admin 8

3.1.6 username terminal

【Command】

username *username* **terminal {all | console | telnet | ssh| web | none}**

【Config-mode】

Global configuration mode

【Parameter】

username: The value is a string of up to 64 characters.

all: Represents all terminals.

console: Indicates the serial port terminal.

telnet: Indicates the telnet terminal.

web: Indicates the web terminal.

ssh: Indicates the ssh terminal.

none: Indicates that the login is not allowed.

【Description】

username terminal command is used to configure the types of terminals that are allowed to log in.

【Example】

#Configure that user test cannot log in to any terminal.

Switch(config)#username test terminal none

User Name:test

Password:****

The user is denied login this terminal.

User Name:

3.1.7 stop

【Command】

stop *username*

【Config-mode】

Privileged user mode

【Parameter】

username: The value is a string of up to 64 characters.

【Description】

stop *username* command is used to force a user offline.

【Example】

Force user test offline.

Switch#stop test

3.2 User Management Monitoring and Debugging Commands

3.2.1 show username

【Command】

show username [*username*]

【Config-mode】

Arbitrary configuration mode.

【Parameter】

username: The value is a string of up to 64 characters.

【Description】

show username this command is used to view user information.

【Example】

#Viewing user information.

Switch(config)#show username

display user information

Terminal type: C=Console, T=Telnet, S=SSH, W=Web

Global Failmax: 8

User Name	Role	Terminal	FailMax	Fail	OnLineMax	OnLine
admin	ADMIN	CTSW	N/A	0	50	2

bala ADMIN CTSW N/A 0 N/A 0

test ADMIN CTSW N/A 0 N/A 0

hero NORMAL CTSW N/A 0 N/A 0

show username display field description

Field	Description
Global Failmax	configuration the maximum number of login failures for all users.
User name	username
Role	User role
Terminal	Allows the login mode of the terminal.
FailMax	Maximum number of login failures.
Fail	Number of failures.
OnLineMax	Maximum number of concurrent online users.
OnLine	Number of online connections.

3.2.2 show username silent

【Command】

show username silent

【Config-mode】

Arbitrary configuration mode.

【Parameter】

None

【Description】

show username silent the command is used to view silent information.

【Example】

#Viewing silent information.

Switch(config)#show username silent

display user silent period information

Silent Time: 10 minutes

User Name State Remaining Silent Time

---

admin Off N/A

bala Off N/A

test Off N/A

hero Off N/A

show username silent display field description

Field	Description
Silent Time	The configured silence time.
User name	username
State	State.Off,On.
Remaining Silent Time	The rest of the silence.

3.3 ssh configuration command

3.3.1 ssh

【Command】

ssh

no ssh

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

ssh command is used to enable the ssh function.

no ssh command is used to disable the ssh function.

【Example】

#Enable the ssh function.

Switch(config)#ssh

3.3.2 ssh port

【Command】

ssh port *port-value*

no ssh

【Config-mode】

Global configuration mode

【Parameter】

port-value: Server port number. The value ranges from 1025 to 65535. The default value is 22.

【Description】

ssh port this command is used to enable the ssh function and change the communication port number.

no ssh command is used to disable the ssh function and restore the default Settings.

By default, the communication port number is 22.

【Example】

#Enable ssh and set the communication port to 1025.

Switch(config)#ssh port 1025

3.3.3 crypto key generate

【Command】

crypto key generate { dss | ecdsa | rsa }

【Config-mode】

Privileged user mode

【Parameter】

dss: Indicates that the dss key is used.

ecdsa: Indicates that the ecdsa key is used.

rsa: Indicates that the rsa key is used.

【Description】

crypto key generate { dss | ecdsa | rsa } command is used to generate a key.

【Example】

#Configure the dss encryption key.

Switch#crypto key generate dss

Generating key, this may take a while...

3.3.4 crypto key zeroize

【Command】

crypto key zeroize { dss | ecdsa | rsa }

【Config-mode】

Privileged user mode

【Parameter】

dss: Indicates that the dss key is used.

ecdsa: Indicates that the ecdsa key is used.

rsa: Indicates that the rsa key is used.

【Description】

crypto key zeroize { dss | ecdsa | rsa } command is used to delete a key.

【Example】

#Delete the dss encryption key.

Switch#crypto key zeroize dss

3.3.5 ssh limit

【Command】

ssh limit *limit-value*

no ssh limit

【Config-mode】

Global configuration mode

【Parameter】

limit-value: Number of sessions. The value ranges from 0 to 5. The default value is 5.

【Description】

ssh limit command is used to set the number of ssh sessions.

no ssh limit command is used to restore default settings.

By default, a maximum of five ssh sessions can be established at the same time

【Example】

#Set the number of ssh sessions to 3.

Switch(config)#ssh limit 3

3.3.6 stop vty

【Command】

stop vty { **all** | *vty-id* }

【Config-mode】

Privileged user mode

【Parameter】

vty-id: Virtual terminal ID. The value is an integer that supports multiple ids, such as 1,3-5.

all: Indicates all virtual terminals.

【Description】

stop vty command is used to forcibly shut down a virtual terminal.

【Example】

#Shut down all virtual terminals.

Switch#stop vty all

Do you want to delete all vty(y/n)?[n]

3.4 ssh monitoring and debugging commands

3.4.1 show ssh

【Command】

show ssh

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show ssh command is used to view the ssh status.

【Example】

#Enable the ssh function to view the ssh status.

Switch(config)#ssh

Switch(config)#show ssh

ssh version : 2.0

ssh state : on

ssh port : 22

ssh rsa key file : unavailable

ssh dss key file : unavailable

ssh ecdsa key file : unavailable

show ssh display field description

Field	Description
ssh version	ssh version
ssh state	ssh state: on、off
ssh port	ssh port number

ssh rsa key file	Status of the rsa key file
ssh dss key file	dss Key file status
ssh ecdsa key file	ecdsa Key file status

3.4.2 show ssh limit

【Command】

show ssh limit

【Config-mode】

Arbitrary configuration mode.

【Parameter】

None

【Description】

show ssh limit command is used to view SSH session information.

【Example】

#View ssh session information.

Switch(config)#show ssh limit

SSH user limit is 5, current is 1.

3.5 telnet configuration command

3.5.1 telnet { enable | disable }

【Command】

telnet { enable | disable }

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

telnet enable command is used to enable the telnet server function.

telnet disable command is used to disable the telnet server function.

The telnet server function is enabled by default.

【Example】

#Enable the telnet server function.

Switch(config)#telnet enable

3.5.2 telnet port

【Command】

telnet port *port-value*

no telnet port

【Config-mode】

Global configuration mode

【Parameter】

port-value: Protocol port number. The value ranges from 1024 to 65535. The default value is 23.

【Description】

telnet port the telnet server port command is used to set the Telnet Server port number.

no telnet port command is used to restore default values.

By default, the telnet sever port number is 23.

【Example】

#Set the telnet server port number to 10240.

Switch(config)#telnet port 10240

3.5.3 telnet limit

【Command】

telnet limit *limit-value*

no telnet limit

【Config-mode】

Global configuration mode

【Parameter】

limit-value: Number of sessions. The value ranges from 0 to 5. The default value is 5.

【Description】

telnet limit command is used to set the maximum number of telnet sessions.

no telnet limit command is used to restore default values.

By default, a maximum of five sessions can be established at the same time.

【Example】

#Configure a maximum of three telnet sessions.

Switch(config)#telnet limit 3

3.5.4 stop vty

【Command】

stop vty { **all** | *vty-id* }

【Config-mode】

Privileged user mode

【Parameter】

vty-id: Virtual terminal ID. The value is an integer that supports multiple ids, such as 1,3-5.

all: Indicates all virtual terminals.

【Description】

stop vty command is used to force a virtual terminal offline.

【Example】

#Shut down all virtual terminals.

Switch#stop vty all

Do you want to delete all vty(y/n)?[n]

3.5.5 telnet ip-address

【Command】

telnet *ip-address*

【Config-mode】

Privileged user mode

【Parameter】

ip-address: The server IP address is in dotted decimal notation and in the format of x.x.x.x.

【Description】

telnet *ip-address* The telnet command is used to remotely connect to the telnet server.

In this command, the device functions as a telnet client.

【Example】

#Remotely connect to the telnet server: 10.2.55.248.

Switch#telnet 10.2.55.248

Trying to connect to 10.2.55.248 ....

3.5.6 telnet6 ipv6-address

【Command】

telnet6 *ipv6-address*

【Config-mode】

Privileged user mode

【Parameter】

ipv6-address: The IPv6 address of the server is in hexadecimal format :x:x:x:x:x.

【Description】

telnet6 The ipv6 telnet server command is used to remotely log in to the device.

In this command, the device functions as an ipv6 telnet client.

【Example】

#Remote connection to ipv6 telnet server: 2001::1.

Switch#telnet6 2001::1

Trying to connect to 2001::1 ...

3.6 Telent Monitoring and debugging commands

3.6.1 show telnet

【Command】

show telnet

【Config-mode】

Arbitrary configuration mode.

【Parameter】

None.

【Description】

show telnet command is used to view the telnet remote connection status and configuration.

【Example】

#View telnet configuration information.

Switch(config)#show telnet

Telnet service port is 23, using port is 23, user limit is 5, current is 0.

3.6.2 show telnet limit

【Command】

show telnet limit

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show telnet limit command is used to view the number of telnet remote connections and logins.

【Example】

#View the maximum number of telnet remote connections and login counts.

Switch(config)#show telnet limit

Telnet user limit is 5, current is 1.login is 1.

3.7 Web configuration command

3.7.1 http

【Command】

http enable [**port** *port-value*]

http disable

【Config-mode】

Global configuration mode

【Parameter】

port-value: Protocol port number. The value ranges from 3 to 65535. The default value is 80.

【Description】

http enable ,these commands are used to enable the http function and configure the port number.

http disable command is used to disable the http function.

【Example】

#Enable the http function and configure port 10240.

Switch(config)#http enable port 10240

3.7.2 http enable ssl

【Command】

http enable ssl [port *port-value*]

http disable

【Config-mode】

Global configuration mode

【Parameter】

port-value: Protocol port number. The value ranges from 3 to 65535. The default value is 80.

【Description】

http enable ssl command is used to enable the https function and configure the port number.

http disable command is used to disable the https function.

【Example】

#Enable the http function and set port number to 10240.

Switch(config)#http enable ssl port 10240

3.7.3 load server-certificate

【Command】

load server-certificate ftp { inet | inet6 } *ip-address filename username password*

load server-certificate tftp { inet | inet6 } *ip-address filename*

【Config-mode】

Privileged user mode

【Parameter】

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters.

username: ftp server user name. The value is a string of 1 to 32 characters.

password: ftp server password. The value is a string of 1 to 32 characters.

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

【Description】

load server-certificate command is used to download the https certificate file.

【Example】

#Use ftp to download the https certificate file.

Switch#load server-certificate ftp inet 192.168.1.111 test.txt test 123

Downloading file...

3.7.4 load private-key

【Command】

load private-key ftp { inet | inet6 } *ip-address filename username password*

load private-key tftp { inet | inet6 } *ip-address filename*

【Config-mode】

Privileged user mode

【Parameter】

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.filename: The name of the file is a string of 1 to 64 characters.

username: ftp server user name. The value is a string of 1 to 32 characters.

password: The value is a string of 1 to 32 characters.

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

【Description】

load private-key command is used to download the https key file.

【Example】

#Use the ftp server to download the https key file.

Switch#load private-key ftp inet 192.168.1.111 test.txt test 123

Downloading file...

3.7.5 http timeout

【Command】

http timeout *time-value*

no http timeout

【Config-mode】

Global configuration mode

【Parameter】

time-value: timeout period,the value ranges from 60 to 36,000 seconds. The default value is 1200 seconds.

【Description】

http timeout *time-value* The web terminal timeout command is used to set the web terminal timeout period.

no http timeout the command is used to restore default settings.

By default, the timeout period of the web terminal is 1200 seconds.

This command applies only to web terminals.

【Example】

#Set the web terminal timeout period to 600 seconds.

Switch(config)#http timeout 600

3.8 Web Monitoring and debugging commands

3.8.1 show http

【Command】

show http

【Config-mode】

Arbitrary configuration mode.

【Parameter】

None

【Description】

show http command is used to view http configuration information.

【Example】

#View http configuration information.

Switch#show http

Web Server status:

Running:TRUE

Port:80

Timeout:1200(s)

show http display field description

Field	Description
Running	Enabled state
Port	Transport layer port number
Timeout	Timeout period

3.9 baud-rate configuration command

3.9.1 baud-rate

【Command】

baud-rate *rate-value*

【Config-mode】

Global configuration mode

【Parameter】

rate-value: Baud rate. The value range is 110-9216000. The default value is 115200.

【Description】

baud-rate *rate-value* this command is used to set the maximum communication rate of a serial port.

There is no delete command. The default is to delete the configuration.

The configuration can be viewed by decompiling.

【Example】

#Set the baud rate of the serial port to 9600.

Switch(config)#baud-rate 9600

Chapter 4 System management

4.1 System Management Configuration Commands

4.1.1 terminal language

【Command】

terminal language { chinese | english }

【Config-mode】

Privileged user mode

【Parameter】

chinese: Indicates that the prompt information of the command line terminal is displayed in Chinese.

english: The prompt information of the command line terminal is displayed in English.

【Description】

terminal language command is used to configure the prompt language of the command line terminal.

When changing the language type of the prompt message, you need to change the coding type of the serial port tool.

【Example】

#The configuration prompt is displayed in english.

Switch#terminal language english

Switch#configure terminal

Switch(config)#interface ?

eth-trunk Ethernet aggregation group

ethernet Ethernet port

internal-interface Internal interface

loopback-interface Loopback interface

range Port list range

supervlan-interface superVLAN interface

vlan-interface VLAN interface

4.1.2 hostname

【Command】

hostname *hostname*

no hostname

【Config-mode】

Global configuration mode

【Parameter】

hostname: The value is a string of up to 64 characters. The default value is Switch.

【Description】

Hostname command is used to configure the system host name.

no hostname command is used to restore default Settings.

By default, the system host name is Switch.

【Example】

#Change the system host name to DUT.

Switch(config)#hostname DUT

DUT(config)#

4.1.3 cls

【Command】

cls

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

cls command is used to clear the screen.

【Example】

#Clear the screen.

Switch#cls

4.1.4 buildrun mode

【Command】

buildrun mode { continue | stop }

【Config-mode】

Privileged user mode

【Parameter】

continue: continue to load the configuration when an error occurs,default action.

stop: stop to load configuration when an error occurs.

【Description】

buildrun mode command is used to configure the handling mode when loading configuration errors occur.

【Example】

#The configuration load continues when it encounters an error.

Switch#buildrun mode continue

4.1.5 line width

【Command】

line width *width-value*

【Config-mode】

Privileged user mode

【Parameter】

width-value: Maximum character count, The value ranges from 78 to 256. The default value is 78.

【Description】

line width command is used to set the maximum number of characters that can be displayed in a line.

【Example】

#Each line can display a maximum of 128 characters.

Switch#line width 128

4.1.6 screen-rows per-page

【Command】

screen-rows per-page *per-page-value*

no screen-rows per-page

【Config-mode】

Privileged user mode

【Parameter】

per-page-value: Number of rows to be displayed per page. The value ranges from 0 to 256. 0 indicates that there is no paging.

【Description】

screen-rows per-page command is used to set the number of lines to be displayed on each page.

no screen-rows per-page command is used to restore default Settings.

By default, 22 lines are displayed per page.

【Example】

#Configure 20 lines per page.

Switch#screen-rows per-page 20

4.1.7 clock set

【Command】

clock set *time-value date-value*

【Config-mode】

Privileged user mode

【Parameter】

time-value: time, format:HH:MM:SS.

date-value: date, format:YYYY/MM/DD.

【Description】

clock set command is used to set the system time.

If the system hardware does not support it, the system time is restored to the default value after the system restarts:1970/01/01 00:00:00

【Example】

#Setting the system time 2022/12/12 10:00:00.

Switch#clock set 10:00:00 2022/12/12

4.1.8 clock timezone

【Command】

clock timezone *timezone-name hours-offset minutes-offset*

no clock timezone

【Config-mode】

Global configuration mode

【Parameter】

timezone-name:Time zone name,The value is a string of 1 to 32 characters.

hours-offset:Offset hour,the value ranges from 23 to 23.

minutes-offset: Offset minute. The value ranges from 0 to 59.

【Description】

clock timezone command is used to configure the time zone.

no clock timezone command is used to restore default settings.

By default, the offset is 8 hours, that is, Beijing time is used. By default, the offset is 8 hours, that is, Beijing time is used.

【Example】

#Configure a time zone named cct: offset 10 hours and 20 minutes.

Switch(config)#clock timezone cct 10 20

4.1.9 reboot

【Command】

reboot

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

Reboot command is used to restart the system immediately.

【Example】

#Restart the system immediately.

Switch#reboot

If you do not save the settings, all changes made will be lost.

Are you sure you want to proceed with the system reboot(y/n)?[n]y

4.1.10 auto-reboot in

【Command】

auto-reboot in hours *hours* **minutes** *minutes*

no auto-reboot

【Config-mode】

Global configuration mode

【Parameter】

hours: Hour, the value is an integer ranging from 0 to 23.

minutes: Minutes, the value is an integer ranging from 0 to 59.

【Description】

auto-reboot in hours command is used to configure the system to automatically restart after a specified time.

no auto-reboot command is used to delete the automatic restart configuration.

auto-reboot in command takes effect only once, does not decompile, and does not save the configuration.

【Example】

#The system restarts automatically one minute after the configuration.

Switch(config)#auto-reboot in hours 0 minutes 1

Switch(config)#

It's time to reload, ready to reboot.....

0

U-Boot 2011.12.(3.6.7.55090) (Jun 07 2022 - 19:46:06)

4.1.11 auto-reboot at

【Command】

auto-reboot at *time [date* | **daily | { fri | mon | sat | sun | thu | tue | wed } weekly**]

no auto-reboot

【Config-mode】

Global configuration mode

【Parameter】

time:time,format:HH:MM:SS.

date:date,format:YYYY/MM/DD.

daily:Every day.

fri weekly: Friday of every week.

mon weekly: Monday of every week.

sat weekly: Saturday of every week.

sun weekly: Sunday of every week.

thu weekly: Thursday of every week.

tue weekly: Tuesday of every week.

wed weekly: Wednesday of every week.

【Description】

auto-reboot at command is used to configure periodic automatic restart of the system.

no auto-reboot command is used to delete a configuration.

The parameter with only time indicates the date of using the system.

When you configure **auto-reboot at time date**,The date must be greater than the current system time, and the interval between the former and the current system time cannot be greater than 180 days.

After the **auto-reboot at** command is configured, if you run the clock set command to change the system time, the **auto-reboot at** configuration is automatically deleted when the interval between the new system time and the restart time is less than 0 seconds or longer than 180 days.

【Example】

#Configure an automatic restart at 12:12:12 every day.

Switch(config)#auto-reboot at 12:12:12 daily

4.2 System Management Monitoring and Debugging Commands

4.2.1 show version

【Command】

show version

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show version command is used to view the system version information.

【Example】

#View the system version.

Switch(config)#show version

Switch Device, Compiled on Wed Sep 21 16:42:36 CST 2022

Software Version V1.8e

BootRom Version V1.0

Hardware Version V1.0

CPLD Version N/A

Processor: 34Kc MIPS 1GHz

Serial No.: 0022559988sbawe

Copyright (C) 2001-2021

All Rights Reserved.

Last reboot is cold reset.

Uptime is 0 weeks, 0 days, 0 hours, 1 minutes

show version display field description

Field	Description
Software Version	Software version
BootRom Version	BootRom version
Hardware Version	Hardware Version
CPLD Version	CPLD version information
Processor	Processor information
Serial No.	Serial number
Copyright	Copyright information

4.2.2 show system

【Command】

show system

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show system command is used to view system information.

【Example】

#View system information.

Switch(config)#show system

system configuration

system description : Switch

system object id : 1.3.6.1.4.1.54367.1.3.32.1

system name : Switch FR-S3128GT

system run time : 04 hour 04 minute 23 second

system location : sample sysLocation factory default

administrator contact : http://

product name : FR-S3128GT

interface of system : 28

show system field description

Field	Description
system description	System description
system object id	Device OID
system name	system name
system run time	System uptime
system location	System location
administrator contact	Contact information
product name	Product name

interface of system	Number of system interfaces

4.2.3 show clock

【Command】

show clock

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show clock command is used to view the current system time.

【Example】

#View the current system time and time zone information.

Switch#show clock

Sun 2022/10/11 15:11:51 CCT 08:00

4.2.4 show auto-reboot

【Command】

show auto-reboot

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show auto-reboot command is used to view the automatic restart configuration.

【Example】

#View the automatic restart configuration.

Switch(config)#show auto-reboot

Auto-reboot setting

Type: durational

Time: 12:12:12 daily

Auto-reboot in 23 hours, 23 minutes and 41 seconds.

show auto-reboot field description

Field	Description
Type	type: at、in
Time	Reboot time

4.2.5 show memory

【Command】

show memory

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show memory command is used to view system memory information.

【Example】

#View system information.

Switch(config)#show memory

Memory information:

Total Memory : 256 MB

Free Memory : 166 MB

show memory field description

Field	Description
Total Memory	Total memory
Free Memory	Available memory

4.2.6 show screen-rows per-page

【Command】

show screen-rows per-page

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show screen-rows per-page command is used to view split screen configuration information.

【Example】

#View split screen configuration information.

Switch#show screen-rows per-page

Screen maximum rows number per page (0 means output all in one page): 20

4.2.7 show line-width

【Command】

show line-width

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show line-width command is used to view the number of characters displayed in each line.

【Example】

#View the number of characters that can be displayed in each line.

Switch#show line width

max chars perline: 78

4.2.8 show tech-support

【Command】

show tech-support { nowait | product-sn }

【Config-mode】

Arbitrary configuration mode

【Parameter】

nowait: All technical support information is displayed at one time.

product-sn: Indicates that product version information is displayed.

Normally, the version information in **show version** is the same as that in **show tech-support product-sn**..The information is different only under certain circumstances: For example, if the customer is using version v1 and requires a new version, but v1 is still used during compilation. To facilitate the differentiation between the version number and the compilation number, the **show version** may be displayed as required by the customer, but the real compilation time is displayed in the **show tech-support product-sn**.

【Description】

show tech-support command is used to view technical support information.

【Example】

#View product information.

Switch(config)#show tech-support product-sn

product-sn: V1.8h-Mon Jan 9 10:41:02 CST 2023

4.2.9 show cpu-utilization

【Command】

show cpu-utilization

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show cpu-utilization command is used to view the idle cpu utilization.

【Example】

#view the idle cpu utilization.

Switch(config)#show cpu-utilization

CPU Information:

CPU Idle : 95 %

4.2.10 show running-config

【Command】

show running-config [*module-name*]

【Config-mode】

Arbitrary configuration mode

【Parameter】

module-name: Module name. For details, see the help information.

【Description】

show running-config command is used to view the decompile configuration, that is the current configuration.

【Example】

#View the decompile configuration.

Switch(config)#show running-config

!LanSwitch BuildRun

enable

configure terminal

![VLAN]

vlan 2-10,1000

exit

interface ethernet 0/0/1

switchport pvid 1000

switchport hybrid untagged vlan 1000

……

4.2.11 show startup-config

【Command】

show startup-config [*module-name*]

【Config-mode】

Arbitrary configuration mode

【Parameter】

module-name: Module name. For details, see the help information.

【Description】

show startup-config command is used to view the configuration that is loaded after the system restarts.

【Example】

#View the startup configuration.

Switch(config)#show startup-config

!LanSwitch BuildRun

enable

configure terminal

![VLAN]

vlan 2-10,1000

exit

interface ethernet 0/0/1

switchport pvid 1000

switchport hybrid untagged vlan

……

Chapter 5 System log management

5.1 System Log Management Configuration Commands

5.1.1 logging

【Command】

logging

no logging

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

logging command is used to enable the log function.

no logging command is used to disable the log function.

By default, the logging function is enabled.

【Example】

#Enable the log function.

Switch(config)#logging

5.1.2 logging sequence-numbers

【Command】

logging sequence-numbers

no logging sequence-numbers

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

logging sequence-numbers command is used to enable the log serial number..

no logging sequence-numbers command is used to disable the log serial number..

By default, the log sequence number is not displayed (disabled).

【Example】

#Indicates the serial number of the enabled log.

Switch(config)#logging sequence-numbers

5.1.3 logging timestamps

【Command】

logging timestamps { notime | uptime | datetime }

no logging timestamps

【Config-mode】

Global configuration mode

【Parameter】

notime: Indicates that the time is not displayed.

uptime: Indicates the system run time.

datetime: Indicates the system time.

The default value is uptime.

【Description】

logging timestamps command is used to set the timestamp type.

no logging timestamps command is used to restore default settings.

The default value is uptime.

【Example】

#Set the log timestamp type to notime.

Switch(config)#logging timestamps notime

5.1.4 terminal monitor

【Command】

terminal monitor

no terminal monitor

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

terminal monitor command is used to enable log output to the terminal.

no terminal monitor command is used to disable log output to the terminal.

By default, the log output to the terminal function is disabled.

This command must be used with the **logging monitor**.

【Example】

#Configure log output to the terminal.

Switch#terminal monitor

5.1.5 logging monitor

【Command】

logging monitor { **all** | *monitor-id* }

no logging monitor { **all** | *monitor-id* }

【Config-mode】

Global configuration mode

【Parameter】

all: Represents all terminals.

monitor-id: Terminal number, the value is an integer ranging from 0 to 5. Indicates serial port terminals, others indicate telnet and ssh terminals.

【Description】

logging monitor command is used to configure the terminal ID for outputting logs.

no logging monitor command is used to restore default Settings.

By default, no terminal ID is configured for outputting logs.

This command needs to be used with **terminal monitor**.

【Example】

#Configure log output to all terminals.

Switch(config)#logging monitor all

5.1.6 logging monitor { all | monitor-id } { level-id | none | level-list }

【Command】

logging monitor { all | *monitor-id* } { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*]

no logging monitor {all | *monitor-id* } **filter**

【Config-mode】

Global configuration mode

【Parameter】

monitor-id: Terminal number,The value is an integer ranging from 0 to 5. 0 indicates the serial port terminal, and others indicate telnet and ssh terminals.

level-id: Log information level. The value ranges from 0 to 7.

none: Indicates that no log information is output.

level-list: Indicates the log information level list.

start-level: Start value of the log level list. The value ranges from 0 to 7.

end-level: End value of the log level list. The value ranges from 0 to 7.

module-name: Module name. For details, see the help information.

【Description】

logging monitor { all | *monitor-id } { level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*] command is used to configure filtering rules for logs that are output to the terminal.

no logging monitor {all | *monitor-id* } **filter** command is used to restore the default Settings.

By default, the level of logs output to the terminal is 0-5 and 7.

【Example】

#Configure the level of the log information output to the terminal to be 0 to 5.

Switch(config)#logging monitor all level-list 0 to 5

5.1.7 logging buffered

【Command】

logging buffered

no logging buffered

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

logging buffered command is used to enable output logs to the buffer.

no logging buffered command is used to disable outputting logs to the buffer.

By default, logs are output to the buffer.

After the device is restarted, logs in the buffer are cleared.

【Example】

#Enable the output log to buffer.

Switch(config)#logging buffered

5.1.8 logging buffered { level-id | none | level-list }

【Command】

logging buffered { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*]

no logging buffered filter

【Config-mode】

Global configuration mode

【Parameter】

level-id: Log information level. The value ranges from 0 to 7.

none: Indicates that no log information is output.

level-list: Indicates the log information level list.

start-level: Start value of the log level list. The value ranges from 0 to 7.

end-level: End value of the log level list. The value ranges from 0 to 7.

module-name: Module name. For details, see the help information.

【Description】

logging buffered { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*] command is used to configure filtering rules for logs output to the buffer.

no logging buffered filter command is used to restore the default settings.

By default, the level of logs output to buffer ranges from 0 to 6.

【Example】

#Configure the level of log information output to the buffer to be 0 to 5

Switch(config)#logging buffer level-list 0 to 5

5.1.9 logging flash

【Command】

logging flash

no logging flash

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

logging flash command is used to enable to output logs to the flash.

no logging flash command is used to restore default Settings.

By default, outputting logs to the flash is disabled.

A large amount of log information is written into the flash,May affect the use,Please use with caution.

【Example】

#The function of outputting logs to the flash is enabled.

Switch(config)#logging flash

5.1.10 logging flash interval

【Command】

logging flash interval *interval-value*

no logging flash interval

【Config-mode】

Global configuration mode

【Parameter】

interval-value: Periodic interval, The value is an integer ranging from 30 to 180, in minutes. The default value is 30.

【Description】

logging flash interval command is used to set the period for outputting logs to the flash.

no logging flash interval command is used to restore default Settings.

By default, the period for outputting logs to the flash is 30 minutes.

After the function of outputting log information to the flash is enabled, the log information is not written to the flash immediately after being generated.Instead, it waits until a certain time to write the log information into flash.A write to flash is triggered at the following conditions:

A.System restart ;

B.Reach time period **logging flash interval** *interval-value* ;

C.The number of logs written reached the specified value: **logging flash msg-number** *msg-number*.

【Example】

#Set the period for outputting logs to the flash to 40 minutes.

Switch(config)#logging flash interval 40

5.1.11 logging flash msg-number

【Command】

logging flash msg-number *msg-number*

no logging flash msg-number

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

logging flash msg-number command is used to configure the number of information that triggers the output of logs to

the flash.

no logging flash msg-number command is used to restore default settings.

By default, the number of trigger logs to be output to the flash is 100.

After the function of outputting log information to the flash is enabled, the log information is not written to the flash immediately after being generated. Instead, the log information is written to the flash at a specific time. A write to flash is triggered at the following three times:

A.System restart ;

B.Reach time period **logging flash interval** *interval-value* ;

C.The number of logs to be written reached the specified value: **logging flash msg-number** *msg-number*.

【Example】

#Set the number of messages that trigger the output of logs to the flash to 200.

Switch(config)#logging flash msg-number 200

5.1.12 logging flash { level-id | none | level-list }

【Command】

logging flash { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*]

no logging flash filter

【Config-mode】

Global configuration mode

【Parameter】

level-id: Log information level. The value ranges from 0 to 7.

none: Indicates that no log information is output.

level-list: Indicates the log information level list.

start-level: Start value of the log level list. The value ranges from 0 to 7.

end-level: End value of the log level list. The value ranges from 0 to 7.

module-name: Module name. For details, see the help information.

【Description】

logging flash { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*] command is used to configure filtering rules for logs to be output to the flash.

no logging flash filter command is used to restore the default Settings.

By default, the level of logs output to the flash ranges from 0 to 6.

【Example】

#Set the level of log information output to flash to 3

Switch(config)#logging flash 3

5.1.13 logging snmp-agent

【Command】

logging snmp-agent

no logging snmp-agent

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

logging snmp-agent command is used to enable the snmp agent to output logs.

no logging snmp-agent command is used to restore default settings.

By default, outputting logs to the snmp agent is disabled.

【Example】

#Enable the snmp agent to output logs.

Switch(config)#logging snmp-agent

5.1.14 logging snmp-agent { level-id | none | level-list }

【Command】

logging snmp-agent { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*]

no logging snmp-agent filter

【Config-mode】

Global configuration mode

【Parameter】

level-id: Log information level. The value ranges from 0 to 7.

none: Indicates that no log information is output.

level-list: Indicates the log information level list.

start-level: Start value of the log level list. The value ranges from 0 to 7.

end-level: End value of the log level list. The value ranges from 0 to 7.

module-name: Module name. For details, see the help information.

【Description】

logging snmp-agent { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*] command is used to configure the log filtering rule for output to snmp agent.

no logging snmp-agent filter command is used to restore the default settings.

By default, the level of snmp logs is 0-6.

【Example】

#Set the level of the logs output to the snmp agent to 5

Switch(config)#logging snmp-agent 5

5.1.15 logging ip-address

【Command】

logging *ip-address*

no logging *ip-address*

【Config-mode】

Global configuration mode

【Parameter】

ip-address: syslog server IP address is in dotted decimal notation and in the format of x.x.x.x.

【Description】

logging *ip-address* command is used to configure the syslog server.

no logging *ip-address* command is used to delete the syslog server.

【Example】

#Configuring the log Server:192.168.1.11.

Switch(config)#logging 192.168.1.111

5.1.16 logging host

【Command】

logging host { **all** | *ip-address* }

no logging host { **all** | *ip-address* }

【Config-mode】

Global configuration mode

【Parameter】

ip-address: syslog server IP address, The value is in dotted decimal notation in the format of x.x.x.x.

all: Indicates all log servers.

【Description】

logging host{ **all** | *ip-address* } command is used to enable you to output logs to the server.

no logging host command is used to delete a configuration.

【Example】

#Enable the input log to the server:192.168.1.11.

Switch(config)#logging host 192.168.1.11

5.1.17 logging facility

【Command】

logging facility [clock1 | clock2 | ftp | kernel | lineprinter | localuse0 | localuse1 | localuse2 | localuse3 | localuse4 | localuse5 | localuse6 | localuse6 | localuse7 | logalert | logaudit | mail | networkknews | ntp | security1 | security2 | syslogd | system | userlevel | uucp]

no logging facility

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

logging facility command is used to set the name of the logging tool.

no logging facility command is used to restore default Settings.

The default recording tool name is localuse7.

【Example】

#Set the logging tool name to security1.

Switch(config)#logging facility security1

5.1.18 logging source

【Command】

logging source { *ip-address* | **loopback-interface** *interfac-id* }

no logging source

【Config-mode】

Global configuration mode

【Parameter】

ip-address: The source address of the log packet,The value is in dotted decimal notation in the format of x.x.x.x.

interface-id: Loopback number,The value ranges from 0 to 1.

【Description】

logging source command is used to configure the source IP address of log packets.

no logging source command is used to restore default settings.

By default, the interface address is used as the source address.

【Example】

#The source IP address of log packets is set to loopback interface 0.

Switch(config)#interface loopback-interface 0

Switch(config-if-loopBackInterface-0)#ip address 2.2.2.2 255.255.255.255

Switch(config-if-loopBackInterface-0)#exit

Switch(config)#logging source loopback-interface 0

5.1.19 logging host { level-id | none | level-list }

【Command】

logging host { **all** | *ip-address* } { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*]

no logging host { **all** | *ip-address* } **filter**

【Config-mode】

Global configuration mode

【Parameter】

ip-address: The source address of the log packet is in dotted decimal notation in the format of x.x.x.x.

level-id: Log information level. The value ranges from 0 to 7.

none: Indicates that no log information is output.

level-list: Indicates the log information level list.

start-level: Start value of the log level list. The value ranges from 0 to 7.

end-level: End value of the log level list. The value ranges from 0 to 7.

module-name: Module name. For details, see the help information.

【Description】

logging host { **all** | *ip-address* } { *level-id* | **none | level-list** *start-level* **to** *end-level* } [**module** *module-name*] command is used to configure filtering rules for logs sent to the server.

no logging host { **all** | *ip-address* } **filter** command is used to restore the default Settings.

By default, the level of logs output to the server ranges from 0 to 6.

【Example】

#Set the level of the log information to 5

Switch(config)#logging host all 5

5.2 System Log Management Monitoring and Debugging Commands

5.2.1 show logging

【Command】

show logging

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show logging command is used to view log configuration information.

【Example】

#View log configuration information.

Switch(config)#show logging

state: on;

logging sequence-numbers: off;

logging timestamps: uptime;

logging language: english;

logging flash msg-number: 100;

logging flash interval: 30 minutes;

logging monitor:

Console: state: off; display: on; 0 logged; 0 lost; 0 overflow.

Telnet 1: state: off; display: off; 0 logged; 0 lost; 0 overflow.

Telnet 2: state: off; display: off; 0 logged; 0 lost; 0 overflow.

Telnet 3: state: off; display: off; 0 logged; 0 lost; 0 overflow.

Telnet 4: state: off; display: off; 0 logged; 0 lost; 0 overflow.

Telnet 5: state: off; display: off; 0 logged; 0 lost; 0 overflow.

logging buffered: state: on; 131 logged; 0 lost; 0 overflow.

logging flash: state: off; 0 logged; 0 lost; 0 overflow.

logging loghost:

192.168.1.111: state: on; 58 logged; 0 lost; 0 overflow.

logging facility: localuse7;logging source: 1.1.1.1;

logging SNMP Agent: state: off; 0 logged; 0 lost; 0 overflow.

show logging field description

Field	Description

state	Status of the log function: on、off
logging sequence-numbers	Log SN Indicates whether the log SN is enabled: on、off
logging timestamps	Timestamp type: notime、uptime、datetime
logging language	Logging language
logging flash msg-number	Number of logs that trigger writing logs to the flash
logging flash interval	Period when logs are written to the flash
logging monitor	Terminal status.
logging buffered	bufferstate
logging flash	flashstate
logging loghost	Configure sending logs to the log server
logging facility	Specifies the name of the logging tool
logging SNMP Agent	snmp agent status

5.2.2 show logging filter

【Command】

show logging filter { **buffered** | **flash** | **host** *ip-address* | **snmp-agent** | **monitor** *monitor-id* }

【Config-mode】

Arbitrary configuration mode

【Parameter】

ip-address: The server IP address is in dotted decimal notation and in the format of x.x.x.x.

monitor-id: Terminal number,The value is an integer ranging from 0 to 5.0 indicates the serial port terminal, and others indicate telnet and ssh terminals.

【Description】

show logging filter command is used to view log filtering rules.

【Example】

#View buffer log filtering rules.

Switch(config)#show logging filter buffered

module name : output level

OAM : 0 1 2 3 4 5 6

DEVICE : 0 1 2 3 4 5 6

UNKNOWN_DISCARD : 0 1 2 3 4 5 6

QOS : 0 1 2 3 4 5 6

MIRROR : 0 1 2 3 4 5 6

PORTSTATS : 0 1 2 3 4 5 6

LACP : 0 1 2 3 4 5 6

STP : 0 1 2 3 4 5 6

MSTP : 0 1 2 3 4 5 6

VLAN : 0 1 2 3 4 5 6

MULTICAST : 0 1 2 3 4 5 6

……

5.2.3 show logging buffered

【Command】

show logging buffered [*level-id* | **level-list** *start-level* **to** *end-level*] [**module** *module-name*]

【Config-mode】

Arbitrary configuration mode

【Parameter】

level-id: Log information level. The value ranges from 0 to 7.

level-list: Indicates the log information level list.

start-level: Start value of the log level list. The value ranges from 0 to 7.

end-level: End value of the log level list. The value ranges from 0 to 7.

module-name: Module name. For details, see the help information.

【Description】

show logging buffered command is used to view logs in the buffer.

【Example】

#View logs in the buffer.

Switch(config)#show logging buffered

1 day 00:55:40: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkDown.

23:57:51: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkUp.

23:57:44: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkDown.

23:56:59: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkUp.

23:56:06: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkDown.

23:54:39: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkUp.

23:54:37: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkDown.

23:54:07: %DEVICE-4-LINKUPDOWN: e0/1/1 LinkUp.

5.2.4 show logging flash

【Command】

show logging flash [*level-id* | **level-list** *start-level* **to** *end-level*] [**module** *module-name*]

【Config-mode】

Arbitrary configuration mode

【Parameter】

level-id: Log information level. The value ranges from 0 to 7.

level-list: Indicates the log information level list.

start-level: Start value of the log level list. The value ranges from 0 to 7.

end-level: End value of the log level list. The value ranges from 0 to 7.

module-name: Module name. For details, see the help information.

【Description】

show logging flash command is used to view flash logs.

【Example】

#View logs in the flash.

Switch(config)#show logging flash

Total logging flash node [0].

Displayed logging flash node [0].

Chapter 6 Software upgrade and configuration file management

6.1 Configuration Management

6.1.1 copy running-config startup-config

【Command】

copy running-config startup-config

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

copy running-config startup-config command is used to save the current configuration to the restart configuration file.

This command overwrites the original startup configuration file. Exercise caution when running this command.

【Example】

#Save the current configuration file.

Switch#copy running-config startup-config

6.1.2 copy startup-config running-config

【Command】

copy startup-config running-config

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

copy startup-config running-config command is used to copy the startup configuration to the current configuration.

Startup configurations that conflict with the current configuration fail to load.

【Example】

#Save the current configuration file.

Switch#copy startup-config running-config

6.1.3 clear startup-config [with user-info]

【Command】

clear startup-config [with user-info]

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

clear startup-config command is used to restore the boot configuration to the default configuration.

clear startup-config with user-info command is used to restore the boot configuration, including the user name configuration, to the default configuration.

Use with caution.

【Example】

#Restore the boot configuration to the default configuration.

Switch#copy startup-config

6.2 Configure management and debugging commands

6.2.1 show running-config

【Command】

show running-config [*module-name*]

【Config-mode】

Arbitrary configuration mode

【Parameter】

module-name:Module name. For details, see the help information.

【Description】

show running-config command is used to view the decompile configuration, that is the current configuration.

【Example】

#View the decompile configuration.

Switch(config)#show running-config

!LanSwitch BuildRun

enable

configure terminal

![VLAN]

vlan 2-10,1000

exit

interface ethernet 0/0/1

switchport pvid 1000

switchport hybrid untagged vlan 1000

……

6.2.2 show startup-config

【Command】

show startup-config [*module-name*]

【Config-mode】

Arbitrary configuration mode

【Parameter】

module-name:Module name. For details, see the help information.

【Description】

show startup-config command is used to view the configuration that is loaded after the system restarts.

【Example】

#View the startup configuration.

Switch(config)#show startup-config

!LanSwitch BuildRun

enable

configure terminal

![VLAN]

vlan 2-10,1000

exit

interface ethernet 0/0/1

switchport pvid 1000

switchport hybrid untagged vlan

……

6.3 file download

6.3.1 load application ftp

【Command】

load application ftp { **inet | inet6** } *ip-address filename username password*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that an ipv6 server is used.

ip-address:Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename:File name, a string of 1 to 64 characters, followed by.bix.

username:ftp server user name. The value is a string of 1 to 32 characters.

password:ftp server password. The value is a string of 1 to 32 characters.

【Description】

load application ftp command is used to download host program files through ftp.

After the file is downloaded, restart the system for the file to take effect.

【Example】

#Use ftp to download the host program file.

Switch#load application ftp inet 192.168.1.111 host.bix test 123

6.3.2 load application tftp

【Command】

load application tftp { **inet | inet6** } *ip-address filename*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: File name, a string of 1 to 64 characters, followed by.bix.

【Description】

load application tftp command is used tftp to download the host program file.

After the file is downloaded, restart the system for the file to take effect.

【Example】

#Use tftp to download the host program file.

Switch#load application tftp inet 192.168.1.111 host.bix

6.3.3 load application xmodem

【Command】

load application xmodem

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

load application xmodem command is used to download the host program file through xmodem.

After the file is downloaded, restart the system for the file to take effect.

【Example】

#Use xmodem to download the host program file.

Switch#load application xmodem

6.3.4 load whole-bootrom ftp

【Command】

load whole-bootrom ftp { **inet** | **inet6** } *ip-address filename username password*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename:The name of the file is a string of 1 to 64 characters. The suffix is.bin.

username:ftp server user name. The value is a string of 1 to 32 characters.

password:ftp server user password. The value is a string of 1 to 32 characters.

【Description】

load whole-bootrom ftp command is used to download the bootrom program through ftp.

After the file is downloaded, restart the system for the file to take effect.

【Example】

#Download the bootrom program file through ftp.

Switch#load whole-bootrom ftp inet 192.168.1.111 uboot.bin test 123

6.3.5 load whole-bootrom tftp

【Command】

load whole-bootrom tftp { **inet** | **inet6** } *ip-address filename*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters. The suffix is.bin.

【Description】

load whole-bootrom tftp command is used to download the bootrom program file by tftp.

After the file is downloaded, restart the system for the file to take effect.

【Example】

#Download the bootrom program file through tftp.

Switch#load whole-bootrom tftp inet 192.168.1.111 uboot.bin

6.3.6 load whole-bootrom xmodem

【Command】

load whole-bootrom xmodem

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

load whole-bootrom xmodem command is used to download the bootrom program file by xmodem.

After the file is downloaded, restart the system for the file to take effect.

【Example】

#Download the bootrom program file using xmodem.

Switch#load whole-bootrom xmodem

6.3.7 load configuration ftp

【Command】

load configuration ftp { **inet** | **inet6** } *ip-address filename username password*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters.

username: ftp server user name. The value is a string of 1 to 32 characters.

password: ftp server password. The value is a string of 1 to 32 characters.

【Description】

load configuration ftp command is used to download the configuration file through ftp.

The downloaded file overwrites the current startup configuration file. Exercise caution when performing this operation.

【Example】

#Use ftp to download the configuration file.

Switch#load configuration ftp inet 192.168.1.111 config.txt test 12

3

Startup config will be updated, are you sure(y/n)? [n]

6.3.8 load configuration tftp

【Command】

load configuration tftp { **inet** | **inet6** } *ip-address filename*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters.

【Description】

load configuration tftp command is used to download a configuration file through tftp.

The downloaded file overwrites the current startup configuration file. Exercise caution when performing this operation.

【Example】

#Use tftp to download the configuration file.

Switch#load configuration tftp inet6 aa:ff::22 config.txt

Startup config will be updated, are you sure(y/n)? [n]

6.3.9 load configuration xmodem

【Command】

load configuration xmodem

【Config-mode】

Privileged user mode

【Parameter】

None

【Description】

load configuration xmodem command is used to download the configuration file by xmodem.

The downloaded file overwrites the current startup configuration file. Exercise caution when performing this operation.

【Example】

#Use xmodem to download the configuration file.

Switch#load configuration xmodem

Startup config will be updated, are you sure(y/n)? [n]

6.4 File upload

6.4.1 upload logging ftp

【Command】

upload logging ftp { **inet | inet6** } *ip-address filename username password*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ip server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters.

username: ftp server user name. The value is a string of 1 to 32 characters.

password: The value is a string of 1 to 32 characters.

【Description】

upload logging ftp command is used to upload log files through ftp.

This effect applies only to logs saved to the flash.

【Example】

#Upload log files through ftp.

Switch#upload logging ftp inet 192.168.1.111 test.txt username password

Uploading syslog file via FTP...

6.4.2 upload logging tftp

【Command】

upload logging tftp { **inet | inet6** } *ip-address filename*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters.

【Description】

upload logging tftp command is used to upload log files through tftp.

This effect applies only to logs saved to the flash.

【Example】

#Upload log files through tftp.

Switch#upload logging tftp inet 192.168.1.111 test.txt

Uploading syslog file via TFTP...

6.4.3 upload configuration ftp

【Command】

upload configuration ftp { **inet** | **inet6** } *ip-address filename username password*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters.

username: ftp server user name. The value is a string of 1 to 32 characters.

password: ftp server password. The value is a string of 1 to 32 characters.

【Description】

upload configuration ftp command is used to upload a configuration file through ftp.

【Example】

#Upload the configuration file through ftp.

Switch#upload configuration ftp inet 192.168.1.111 config.txt username pwd

Uploading config file...

6.4.4 upload configuration tftp

【Command】

upload configuration tftp { **inet** | **inet6** } *ip-address filename*

【Config-mode】

Privileged user mode

【Parameter】

inet: Indicates that the ip server is used.

inet6: Indicates that the ipv6 server is used.

ip-address: Server address. If inet is selected, the format is x.x.x.x. If inet6 is selected, the format is x:x:x:x:x.

filename: The name of the file is a string of 1 to 64 characters.

【Description】

upload configuration tftp command is used to upload a configuration file through tftp.

【Example】

#Upload the configuration file through tftp.

Switch#upload configuration ftp inet 192.168.1.111 config.txt

Uploading config file...

Chapter 7 SNTP client

7.1 SNTP client configuration command

7.1.1 sntp client

【Command】

sntp client

no sntp client

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

sntp client this command is used to enable the sntp client function.

no sntp client this command is used to disable the sntp client function.

By default, the sntp client function is disabled.

【Example】

#Enable the sntp client function.

Switch(config)#sntp client

7.1.2 sntp client mode

【Command】

sntp client mode { anycast | broadcast | multicast | unicast }

no sntp client mode

【Config-mode】

Global configuration mode

【Parameter】

anycast: Indicates the arbitrary broadcast mode.

broadcast: Indicates the broadcast mode.

multicast: Indicates the multicast mode.

unicast: Indicates unicast mode.

【Description】

sntp client mode command is used to set the working mode of the sntp client.

no sntp client mode command is used to restore the default mode.

By default, sntp clients work in broadcast mode.

【Example】

#Set the working mode of the sntp client to unicast.

Switch(config)#sntp client mode unicast

7.1.3 sntp client authenticate

【Command】

sntp client authenticate

no sntp client authenticate

【Config-mode】

Global configuration mode

【Parameter】

None

【Description】

sntp client authenticate command is used to enable the MD5 authentication function on sntp clients.

no sntp client authenticate command is used to restore default values.

By default, the sntp client authentication function is disabled. After md5 authentication is enabled, the sntp client receives

only authenticated packets.

【Example】

#The sntp client authentication function is enabled.

Switch(config)#sntp client authenticate

7.1.4 sntp client authentication-key

【Command】

sntp client authentication-key *key-id* **md5** *key-value*

no sntp client authentication-key *key-id*

【Config-mode】

Global configuration mode

【Parameter】

key-id: Authentication key number. Value range: 1 to 4294967295.

md5: Indicates md5 authentication.

key-value: Authentication password, a string of 1 to 16 characters.

【Description】

sntp client authentication-key command is used to configure SNTP authentication keys.

no sntp client authenticate command is used to delete SNTP authentication keys.

【Example】

#Set the sntp md5 authentication key to 1234.

Switch(config)#sntp client authentication-key 1 md5 1234

7.1.5 sntp client broadcastdelay

【Command】

sntp client broadcastdelay *delay-value*

no sntp client broadcastdelay

【Config-mode】

Global configuration mode

【Parameter】

delay-value: The value ranges from 1 to 9999. The default value is 3, in microseconds.

【Description】

sntp client broadcastdelay command is used to set the broadcast transmission delay.

no sntp client broadcastdelay command is used to restore default Settings.

By default, the transmission delay is 3ms.

Broadcast transmission delay is required only when the sntp client works in broadcast or multicast mode. The local system time of the sntp client is the time obtained from the server plus the transmission delay.

【Example】

#Set the broadcast delay to 100 microseconds.

Switch(config)#sntp client broadcastdelay 100

7.1.6 sntp client poll-interval

【Command】

sntp client poll-interval *interval-value*

no sntp client poll-interval

【Config-mode】

Global configuration mode

【Parameter】

interval-value: Polling interval. The value ranges from 64 to 1024. The default value is 1000, in seconds.

【Description】

sntp client poll-interval command is used to configure the polling interval.

no sntp client poll-interval command is used to restore default settings.

By default, the polling interval is 1000 seconds.

The configuration rules are:Polling time (poll-interval) >= (Number of retransmit(retransmit） +1) * retransmit interval(retransmit-interval).

The polling interval takes effect only when the sntp client works in unicast or anycast mode.

【Example】

#Set the polling interval to 200 seconds.

Switch(config)#sntp client poll-interval 200

7.1.7 sntp client retransmit

【Command】

sntp client retransmit *retransmit-value*

no sntp client retransmit

【Config-mode】

Global configuration mode

【Parameter】

retransmit-value: retransmit times. The value ranges from 1 to 10. The default value is 3.

【Description】

sntp client retransmit command is used to set the number of retransmit times.

no sntp client retransmit command is used to restore default Settings.

By default, the number of retransmit times is three.

The configuration rules are:Polling interval（poll-interval） >= （Number of retransmit(retransmit）+1) * Retransmit interval（retransmit-interval）.

The timeout retransmit mechanism takes effect only when the sntp client works in unicast or arbitrary multicast mode.

【Example】

#Set the retransmission times to five.

Switch(config)#sntp client retransmit 5

7.1.8 sntp client retransmit-interval

【Command】

sntp client retransmit-interval *interval-value*

no sntp client retransmit-interval

【Config-mode】

Global configuration mode

【Parameter】

interval-value: Retransmit interval,The value ranges from 3 to 30. The default value is 30, expressed in seconds.

【Description】

sntp client retransmit-interval command is used to configure the retransmit interval.

no sntp client retransmit-interval command is used to restore default Settings.

By default, the interval for retransmit is 30 seconds.

The configuration rules are:Polling interval（poll-interval） >= （Number of retransmit(retransmit）+1) * Retransmit interval（retransmit-interval）.

【Example】

#Set the retransmission interval to 20 seconds.

Switch(config)#sntp client retransmit-interval 20

7.1.9 sntp client summer-time dayly

【Command】

sntp client summer-time dayly *start-month start-day start-timeend-month end-day end-time*

no sntp client summer-time

【Config-mode】

Global configuration mode

【Parameter】

start-month: Starting month,the value range is1-12.

start-day: Starting date,the value ranges from 1 to 31.

start-time: Start time,The value range is 00:00:00 - 23:59:59,the format is HH:MM:SS.

end-month: End month. The value ranges from 1 to 12.

end-day: End day. The value ranges from 1 to 31.

end-time: End time,The value ranges from 00:00:00 to 23:59:59. The format is HH:MM:SS.

【Description】

sntp client summer-time dayly command is used to configure the DST by date.

no sntp client summer-time command is used to delete the DST configuration.

【Example】

#Configure daylight saving Time (DST) by date.

Switch(config)#sntp client summer-time dayly 9 30 10:00:00 11 10 12:12:12

7.1.10 sntp client summer-time weekly

【Command】

sntp client summer-time weekly *start-month start-week* { **fri | mon | sat | sun | thu | tue | wed** } *start-time end-month end-week* { **fri | mon | sat | sun | thu | tue | wed** } *end-time*

no sntp client summer-time

【Config-mode】

Global configuration mode

【Parameter】

start-month: Start month,The value ranges from 1 to 12.

start-week: Start of week,The value ranges from 1 to 5.

fri: friday .

mon: monday

sat: saturday

sun: sunday

thu: thursday

tue: tuesday

wed: wednesday

start-time: Start time, The value range is00:00:00-23:59:59,the format isHH:MM:SS.

end-month: End month, The value range is 1-12.

end-week: End of week, The value range is 1-5.

end-time: End time, The value range is00:00:00-23:59:59,the format is HH:MM:SS.

【Description】

sntp client summer-time daily command is used to configure the daylight saving time (DST) by week.

no sntp client summer-time command is used to delete the DST.

【Example】

#Configure the DST on a weekly basis.

Switch(config)#sntp client summer-time weekly 10 1 Sat 00:00:00 12 2 Fri 23:59:59

7.1.11 sntp client valid-server

【Command】

sntp client valid-server *ip-address wildcard-value*

sntp client valid-server

【Config-mode】

Global configuration mode

【Parameter】

ip-address: The IP address that is allowed to access,The value is in dotted decimal notation in the format of x.x.x.x.

wildcard-value: wildcard-mask,value range 0.0.0.0-255.255.255.255.

【Description】

sntp client valid-server command is used to configure valid SNTP server.

no sntp client valid-server command is used to delete configuration.

When an sntp client works in broadcast or multicast mode, it trusts and receives protocol packets from any sntp server by default.If there is a malicious server on the network that provides incorrect time, the local time cannot be synchronized to the standard time.After a legitimate server list is configured on the sntp client, the client receives only packets whose source addresses are in the legitimate server list, which improves security.

【Example】

#Configure the sntp server.

Switch(config)#sntp client valid-server 192.168.1.111 0.0.0.255

7.1.12 sntp trusted-key

【Command】

sntp trusted-key *key-id*

no sntp trusted-key

【Config-mode】

Global configuration mode

【Parameter】

key-id: Authentication key number. Value range: 1 to 4294967295.

【Description】

sntp trusted-key command is used to configure a trusted key ID.

no sntp trusted-key command is used to delete a key.

When the sntp client works in multicast and broadcast mode, the trusted-key value must be equal to the authentication-key value.

【Example】

#Set the trusted key ID to 1.

Switch(config)#sntp trusted-key 1

7.1.13 sntp server key

【Command】

sntp server key *key-id*

no sntp server key

【Config-mode】

Global configuration mode

【Parameter】

key-id: Authentication key number. Value range: 1 to 4294967295.

【Description】

sntp server key command is used to set the key ID for the server.

no sntp server key command is used to delete a key.

【Example】

#Specify the key ID of the server.

Switch(config)#sntp server key 1

7.1.14 sntp server

【Command】

sntp server *ip-address*

no sntp server

【Config-mode】

Global configuration mode

【Parameter】

ip-address: The server IP address is in dotted decimal notation and in the format of x.x.x.x.

【Description】

sntp server command is used to set the IP address of the primary server.

no sntp server command is used to delete the configuration of the primary server.

If the sntp client works in unicast mode, you must configure the specified sntp server.

【Example】

#Set the IP address of the primary sntp server to 192.168.1.55.

Switch(config)#sntp server 192.168.1.55

7.1.15 sntp server backup

【Command】

sntp server backup *ip-address*

no sntp server backup

【Config-mode】

Global configuration mode

【Parameter】

ip-address: Server IP address, In dotted decimal notation, the format is:x.x.x.x.

【Description】

sntp server backup command is used to set the backup server.

no sntp server backup command is used to delete backup server configurations.

【Example】

#Specify the IP address of the sntp backup server.

Switch(config)#sntp server backup 192.168.1.101

7.1.16 sntp client mode anycast key

【Command】

sntp client mode anycast *key key-id*

no sntp client mode anycast key

【Config-mode】

Global configuration mode

【Parameter】

key-id: Authentication key number. Value range: 1 to 4294967295.

【Description】

sntp client mode anycast key command is used to configure the sntp client to work in any multicast mode and the key ID to be used.

no sntp client mode command is used to restore the default mode.

By default, sntp clients work in broadcast mode.

【Example】

#The configuration works in anycast mode and the authentication key ID is 1.

Switch(config)#sntp client mode anycast key 1

7.2 SNTP client Monitoring and debugging commands

7.2.1 show sntp client

【Command】

show sntp client

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show sntp client command is used to view configuration information.

【Example】

#Check sntp client information when working in unicast mode.

Switch(config)#sntp client mode unicast

Switch(config)#sntp server 192.168.1.112

Switch(config)#show sntp client

Clock state : synchronized Current mode : unicast

Use server : 192.168.1.112 State : idle

Server state : synchronized Server stratum : 1

Retrans-times: 3 Retrans-interval: 30s

Authenticate : disable PrimaryServer: 192.168.1.112

Backup Server: 0.0.0.0 Poll interval : 1000s

Last synchronized time: Wed Oct 19 09:38:11 2022

Last received packet's originateTime: Wed Oct 19 09:38:10 2022

Summer-time is not set.

show sntp client display field description

Field	Description
Clock state	Clock state: unsynchronized、synchronized
Current mode	Working mode: anycast、unicast、broadcast、 multicast
Use server	Server address

Retrans-times	Timeout retransmission times
Retrans-interval	Timeout retransmission interval
Authenticate	Authentication status: disable、enable
PrimaryServer	IP address of the primary server
Backup Server	IP address of the backup server
Poll interval	Polling interval
Last synchronized time	Latest synchronization time
Last received packet's originateTime	The time of the last packet received

7.2.2 show sntp client summer-time

【Command】

show sntp client summer-time

【Config-mode】

Arbitrary configuration mode

【Parameter】

None

【Description】

show sntp client summer-time command is used to view the SNTP Daylight Saving Time (DST) status.

【Example】

#View sntp Daylight saving Time.

Switch(config)#show sntp client summer-time

type: dayly

Start Time: Oct 10, 10:10:10

End Time: Dec 12, 12:12:12

It is in summer-time now.

show sntp client summer-time display field description

Field	Description
type	Daylight saving time type: dayly、weekly
Start Time	Start time
End Time	end time

Chapter 8 Ethernet Port

8.1 Ethernet Port Configure Commands

8.1.1 interface ethernet

【command】

interface ethernet *port-id*

【config-mode】

Global configuration mode

【parameter】

port-id: port number, string format: device number/slot number/port number, such as 0/0/1.

【description】

interface ethernet command is used to enter port configuration mode

【example】

Enter the configuration mode of port 1

switch#configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#

8.1.2 interface eth-trunk

【command】

interface eth-trunk *id*

no interface eth-trunk *id*

【config-mode】

Global configuration mode

【parameter】

id: aggregation group ID. The value ranges from 1 to 16.

【description】

interface eth-trunk command is used to enter the aggregation group configuration mode.

no interface eth-trunk command is used to delete an aggregation group.

Configuring the interface eth-trunk id command for the first time will create the aggregation group and enter configuration mode, and then only enter configuration mode without repeating the creation.

【example】

Create and enter the configuration mode of aggregation group 2

switch#configure terminal

switch(config)#interface eth-trunk 2

switch(config-if-eth-trunk-2)#

8.1.3 interface range

【command】

interface range ethernet *port-id* **[to] ethernet** *port-id*

【config-mode】

Global configuration mode

【parameter】

to: Continuous port .

port-id: port number. string format: device number/slot number/port number, such as 0/0/1.

【description】

interface range command is used to enter multiple port configuration mode.

【example】

Enter the configuration mode for ports 1-10 and 15.

switch#configure terminal

switch(config)#interface range ethernet 0/0/1 to ethernet 0/0/10 ethernet 0/0/15

8.1.4 description

【command】

description *description*

no description

【config-mode】

Port configuration mode

【parameter】

string: Port description. A maximum of 128 characters ,cannot be included the character of ?

【description】

description command is used to configure port description .

no description command is used to delete the description of port.

By default, no port description is configured.

【example】

Set the description of port ethernet 0/0/1 to port1

switch#configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#description port1

switch(config-if-ethernet-0/0/1)#

8.1.5 speed

【command】

speed { auto | 10 | 100 | 1000 | 10000 }

no speed

【config-mode】

Port configuration mode

【parameter】

10: set a rate of 10Mbps

100: set a rate of 100Mbps

1000: set a rate of 1000Mbps

10000: set a rate of 10000Mbps

auto: represents the automatic negotiation mode

【description】

speed command is used to set the rate of an Ethernet port.

no speed command is used to restore the default rate.

The default is auto. If "Port id does not support new configuration." is displayed,means the system does not support new configuration.

When the rate or duplex mode is not consistent between the local end and the peer, it will negotiate according to the IEEE 802.3 standard.

For the electrical port, the rate is set to match the rate of the peer Ethernet port;For the optical port, the rate is set so that it matches the rate of the optical module inserted on the Ethernet port.

Notice:

The rate of an Ethernet port requires duplex mode to operate. The rate and duplex mode supported by an Ethernet port depend on the port type and medium type.

【example】

Set the ethernet 0/0/1 port rate to 100 Mbit/s.

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#speed 100

8.1.6 duplex

【command】

duplex { auto | full | half }

no duplex

【config-mode】

Port configuration mode

【parameter】

auto: Auto negotiation mode: The duplex mode of an Ethernet port is automatically negotiated between the local and peer Ethernet interfaces.

full: Full duplex mode, the Ethernet port can send and receive packets at the same time.

half: The half-duplex mode an Ethernet port can only receive or send packets at a certain time, not at the same time.

【description】

duplex command is used to configure Ethernet interface duplex mode.

no duplex command is used to restore the default value of duplex mode.

The default is auto. If "Port id does not support new configuration." is displayed, means that the system does not support new configuration.

When the rate or duplex mode is not consistent between the local end and the peer, it will negotiate according to the IEEE 802.3 standard.

Notice:

The rate of an Ethernet port requires duplex mode to operate. The rate and duplex mode supported by an Ethernet port depend on the port type and medium type.

【example】

Set the duplex mode of port ethernet 0/0/1 to auto-negotiation mode

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#duplex auto

8.1.7 priority

【command】

priority *value*

no priority

【config-mode】

Port configuration mode

【parameter】

value: Priority value, the value range is 0-7, the default is 0, and the higher the value, the higher the priority.

【description】

priority *value* command is used to set the priority of a port.

no priority command is used to restore the default value of 0.

If a port receives a packet without a VLAN Tag, the device adds PVID and port priority to it when forwarding.

【example】

Configure port ethernet 0/0/1 with priority 1

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#priority 1

switch(config-if-ethernet-0/0/1)#

8.1.8 ingress filtering

【command】

ingress filtering

no ingress filtering

【config-mode】

Port configuration mode

【parameter】

None

【description】

ingress filtering command is used to enable the ingress packet filtering function.

no ingress filtering command is used to disable ingress packet filtering.

By default, the port has enabled ingress packet filtering.

【example】

Enable the ingress packet filtering function of interface ethernet 0/0/1

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)# ingress filtering

switch(config-if-ethernet-0/0/1)#

8.1.9 ingress acceptable-frame

【command】

ingress acceptable-frame { all | tagged | untagged }

no ingress acceptable-frame

【config-mode】

Port configuration mode

【parameter】

all: All packets.

tagged: Packets with vlan tag.

untagged: Packets without valn tag

【description】

ingress acceptable-frame all command is used to configure the type of tagged and untagged packets that a port can receive.

ingress acceptable-frame tagged command is used to configure the port to receive only tagged packet types.

ingress acceptable-frame untagged command is used to configure the port to receive only untagged packet type.

no ingress acceptable-frame The command is used to restore default Settings.

The default value is "all", that is, all packets of the tagged or untagged type are received.

【example】

Configure port ethernet 0/0/1 to receive all packet types

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#ingress acceptable-frame all

8.1.10 switchport link-type

【command】

switchport link-type { access | hybird | trunk }

no switchport link-type

【config-mode】

Port configuration mode

【parameter】

access: Configure the port as the Access type. This type of port can belong to only one vlan and the egress packets are untagged.

hybrid: Configure the port as the hybrid type. This type of port can belong to multiple vlans and the egress packets are untagged ortagged.

trunk: Configure the port as the trunk type. This type of port can belong to multiple vlans and the egress packets are untagged ortagged

【description】

switchport link-type commands is used to configure the port link type.

no switchport link-type command is used to restore default Settings.

By default, the port link type is hybrid.

【example】

Set the link type of port ethernet 0/0/1 to trunk

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#switchport link-type trunk

8.1.11 switchport hybrid

【command】

switchport hybrid { tagged | untagged } vlan { *vlan-list* | **all** }

no switchport hybrid vlan { *vlan-list* | **all** }

【config-mode】

Port configuration mode

【parameter】

untagged: means that packets are forwarded out of this port without a vlan tag.

tagged: means that packets are forwarded out of this port keep its vlan tag.

vlan-list: Vlan list, The VLAN ID ranges from 1 to 4094. The VLAN list contains one or multiple VLAN ids. Discontinuous VLAN ids are separated by commas (,). Consecutive VLAN ids are connected with hyphens (-).

【description】

switchport hybrid command is used to configure hybrid port to join the VLAN.

no switchport hybrid command is used to configure the VLAN that the hybrid port exits.

By default, the hybrid port joins VLAN 1 untagged.

When configuring the hybrid port to join or exit the VLAN, ensure that the link type of the port is hybrid, otherwise an error message will be output

【example】

Configure hybrid port ethernet 0/0/1 to join VLAN 2 untagged and VLAN 3-4 tagged.

switch #configure terminal

switch(config)# interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#switchport mode hybrid

switch(config-if-ethernet-0/0/1)#switchport hybrid untagged vlan 2

switch(config-if-ethernet-0/0/1)#switchport hybrid tagged vlan 3-4

8.1.12 switchport pvid

【command】

switchport pvid *vlan-id*

no switchport pvid

【config-mode】

Port configuration mode

【parameter】

vlan-id: Vlan list, integer format, range from 1 to 4094.

【description】

switchport pvid *vlan-id* command is used to configure the port PVID.

no switchport pvid command is used to restore default settings.

By default, the port PVID is 1.

The vlan-id must be created first, otherwise it will fail to configure and be prompted.

【example】

Configure port 0/0/2 pvid to vlan 2.

switch #configure terminal

switch(config)# interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#switchport pvid 2

8.1.13 shutdown

【command】

shutdown

no shutdown

【config-mode】

Port configuration mode

【parameter】

None

【description】

shutdown command is used to disable a port.

no shutdown command is used to enable a port.

By default, the port is enabled.

while an interface is disabled, the interface status becomes unavailable. When an interface is enabled, the interface state does not become available immediately, its depending on other constraints.

【example】

Disable or enable port ethernet 0/0/1

switch#configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#shutdown

switch(config-if-ethernet-0/0/1)#no shutdown

8.1.14 mtu

【command】

mtu *value*

no mtu

【config-mode】

Port configuration mode

【parameter】

value: Jumbo frame length value, integer form, The value ranges from 1522 to 12288, unit is Byte.

【description】

mtu value command is used to set the maximum jumbo frame length that can be forwarded.

no mtu command is used to restore the default configuration.

By default, the maximum jumbo frame length that can be forwarded is 12288.

【example】

Set the mtu value of port ethernet 0/0/1 to 1500

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#mtu 1580

8.1.15 flow-control

【command】

flow-control

no flow-control

【config-mode】

Port configuration mode

【parameter】

None

【description】

flow-control command is used to enable the traffic control function .

no flow-control command is used to disable the traffic control function .

By default, traffic control is disabled.

【example】

Enable port 0/0/1 flow control function.

switch(config-if-ethernet-0/0/1)#flow-control

8.1.16 vct run

【command】

vct run

【config-mode】

Global configuration mode/Port configuration mode

【parameter】

None

【description】

vct run the command is used to detect the cable status of the device port.

Run the **vct run** command in Global configuration mode,will detect all the cable status of the port;

Run the **vct run** command in port configuration mode,will detect the cable status of current port.

Notice:

The following cable status/faults can be detected using the VCT:

SHORT: Short circuit, in which's two or more wires short together.

OPEN: Open circuit means that the cable in the network cable may be broken.

NORMAL: Indicates that the network cable is connected normally.

LOCATE: Distance between the faulty location and the switch device, When NORMAL, it represents the total length of the line(unit: m).

【example】

#Run cable detection at the port 0/0/46

switch#configure terminal

switch(config)#interface e 0/0/46

switch(config-if-ethernet-0/0/46)#vct run

Port 0/0/46 vct status:

	pair1	pair2	pair3	pair4
status:	NORMAL	NORMAL	NORMAL	NORMAL
locate:	2	2	2	2

8.1.17 loopback internal

【command】

loopback internal

【config-mode】

Global configuration mode/ Port configure mode

【parameter】

None

【description】

loopback internal command is used to enable internal loopback test.

By default, loopback test is disabled.

【example】

#Run the internal loopback test on interface ethernet

switch#configure terminal

switch(config)#interface ethernet 0/0/46

switch(config-if-ethernet-0/0/46)#loopback internal

Port 0/0/46 internal looptest successfully.

8.1.18 loopback external

【command】

loopback external

【config-mode】

Global configuration mode/ Port configure mode

【parameter】

None

【description】

loopback external command is used to enable the external loopback test functionality.

By default, the external loopback test is disable

【example】

#Run the external loopback test at interface ethernet 0/0/46

switch#configure terminal

switch(config)#int ethernet 0/0/46

switch(config-if-ethernet-0/0/46)#loopback external

8.2 Ethernet Port Debug Commands

8.2.1 show interface

【command】

show interface [ethernet *port-id*]

【config-mode】

All configure mode

【parameter】

port-id: port number,string format: device number/slot number/port numbe,such as 0/0/1.

【description】

show interface command is used to view the detail information about the port.

【example】

View the detail information about the port.

switch#show interface

Gigabit Ethernet e0/0/1 current state: enabled, link state: down

Time duration of linkup: 00 second

Hardware address: 44:18:47:80:12:ae

Set speed: auto, actual speed: unknown, duplex mode: unknown

Current port type: 1000BASE-T

Port priority: 0

Flow control: disabled

Broadcast storm control target rate: disabled

Multicast storm control target rate: disabled

Unicast storm control target rate: disabled

Port PVID: 1

Port link-type: hybrid

Tagged VLAN ID

Untagged VLAN ID : 1

Input : 0 packets, 0 bytes

0 broadcasts, 0 multicasts, 0 unicasts

Output : 0 packets, 0 bytes

0 broadcasts, 0 multicasts, 0 unicasts

……

Parameter descriptions of "show interface"

Parameter	Description
current state	Port status:disabled、enabled
link state	Port current status: up、down
Time duration of linkup	The port up time
Hardware address	MAC address
Set speed	Set the port's rate
actual speed	The actual rate of the interface
duplex mode	Current duplex mode
Current port type	Current port type
Port priority	Port priority
Flow control	Flow control status
Broadcast storm control target rate	Broadcast storm control target rate
Multicast storm control target rate	Multicast storm control target rate
Unicast storm control target rate	Unicast storm control target rate
Port PVID	Port PVID
Port link-type	Port current link-type: hybrid、access、trunk
Tagged VLAN ID	The list of tagged vlan

Parameter	Description
Untagged VLAN ID	The list of tagged vlan
Input	Receive package statistics
Output	Send package statistics

8.2.2 show interface brief

【command】

show interface brief [ethernet *port-id*]

【config-mode】

Any configure mode

【parameter】

port-id: port number,string format: device number/slot number/port number,such as 0/0/1.

【description】

show interface brief command is used to view the brief information about the port.

【example】

View the brief information about the port

switch#show interface brief

Port	Desc	Link	shutdn	Speed	Pri	PVID	Mode	TagVlan	UtVlan
e0/0/1		down	false	auto	0	1	hyb		1
e0/0/2		down	false	auto	0	1	hyb		1
e0/0/3		down	false	auto	0	1	hyb		1
e0/0/4		down	false	auto	0	1	hyb		1
e0/0/5		down	false	auto	0	1	hyb		1

e0/0/6 down false auto 0 1 hyb 1

e0/0/7 down false auto 0 1 hyb 1

……

Total entries: 28.

Parameter instructions of "show interface brief"

Parameter	Description
Port	Port number
Desc	Port Description
Link	Port link up status
shutdn	Port Management status
Speed	Port speed
Pri	Port priority
PVID	PVID
Mode	Port link type: access、hybrid、trunk
TagVlan	The list of tagged vlan
UtVlan	The list of untagged vlan
Total entries	statistics

8.2.3 clear interface

【command】

clear interface [ethernet *port-id*]

【config-mode】

Global configuration mode/Port configuration mode

【parameter】

port-id: port number,string format: device number/slot number/port numbe,such as 0/0/1.

【description】

clear interface command is used to clear port statistics.

【example】

Clear all ports statistics..

switch(config)#clear interface

clear interface ethernet ethernet0/0/1 statistics..

switch(config)#clear interface ethernet 0/0/1

8.2.4 show statistics interface

【command】

show statistics interface [brief | ethernet *port-id*]*

【config-mode】

Any

【parameter】

port-id: port number,string format: device number/slot number/port numbe,such as 0/0/1.

【description】

show statistics interface command is used to view the brief (detail) information about the port statistics.

【example】

View the statistics on port 0/0/1

switch(config)#show statistics interface ethernet 0/0/1

Port number : e0/0/1

last 5 minutes input rate 0 bits/sec, 0 packets/sec

last 5 minutes output rate 0 bits/sec, 0 packets/sec

64 byte packets:0

65-127 byte packets:0

128-255 byte packets:0

256-511 byte packets:0

512-1023 byte packets:0

1024-1518 byte packets:0

0 packets input, 0 bytes , 0 discarded packets

0 unicasts, 0 multicasts, 0 broadcasts

0 input errors, 0 FCS error, 0 symbol error, 0 false carrier

0 runts, 0 giants

0 packets output, 0 bytes, 0 discarded packets

0 unicasts, 0 multicasts, 0 broadcasts

0 output errors, 0 deferred, 0 collisions

0 late collisions

Total entries: 1.

8.2.5 show statistics dynamic

【command】

show statistics dynamic { eth-trunk | interface }

【config-mode】

Any

【parameter】

eth-trunk: Aggregate port.

interface: Normal port.

【description】

show statistics dynamic interface command is used to view real-time statistics of all ports.

show statistics dynamic eth-trunk command is used to view the statistics information of aggregation port.

Run this command to view the dynamic statistics of a port.The dynamic statistics are automatically refreshed every 5 seconds.

In the display information, press 0 to clear statistics, press U to roll back to the previous page, press D to display the next page, and press Enter to exit the view

【example】

View real-time statistics of all ports

switch(config)#show statistics dynamic interface

Port Statistics Sun Feb 11 09:12:13 1970

port	link Status	Tx Pkt Count	Tx Byte Count	Rx Pkt Count	Rx Byte Count	Rx Bcast	Rx Mcast
e0/0/1	down	0	0	0	0	0	0
e0/0/2	down	0	0	0	0	0	0
e0/0/3	down	0	0	0	0	0	0

e0/0/4 up 4265 646159 10893 11183444 40 5

e0/0/5 down 0 0 0 0 0 0

e0/0/6 down 0 0 0 0 0 0

e0/0/7 down 0 0 0 0 0 0

e0/0/8 up 10893 11183444 4337 650767 346 703

e0/0/9 down 0 0 0 0 0 0

e0/0/10 down 0 0 0 0 0 0

e0/0/11 down 0 0 0 0 0 0

e0/0/12 down 0 0 0 0 0 0

e0/0/13 down 0 0 0 0 0 0

e0/0/14 down 0 0 0 0 0 0

e0/0/15 down 0 0 0 0 0 0

e0/0/16 down 0 0 0 0 0 0

e0/0/17 down 0 0 0 0 0 0

==========0->Clear Counters U->page up D->page down CR->exit==========

Notes:If you see a E number, you can use the command "line width" to get more

information.

8.2.6 show statistics eth-trunk

【command】

show statistics eth-trunk *id*

【config-mode】

Any

【parameter】

id: Aggregate group number, integer form, range from 1-16.

【description】

show statistics eth-trunk *id* command is used to view aggregated group statistics.

【example】

View statistics of aggregated group 1

switch(config)#show statistics eth-trunk 1

Channel group : 1

last 5 minutes input rate 0 bits/sec, 0 packets/sec

last 5 minutes output rate 0 bits/sec, 0 packets/sec

64 byte packets:0

65-127 byte packets:0

128-255 byte packets:0

256-511 byte packets:0

512-1023 byte packets:0

1024-1518 byte packets:0

0 packets input, 0 bytes , 0 discarded packets

0 unicasts, 0 multicasts, 0 broadcasts

0 input errors, 0 FCS error, 0 symbol error, 0 false carrier

0 runts, 0 giants

0 packets output, 0 bytes, 0 discarded packets

0 unicasts, 0 multicasts, 0 broadcasts

0 output errors, 0 deferred, 0 collisions

0 late collisions

Total entries: 1.

8.2.7 show cpu-statistics

【command】

show cpu-statistics [ethernet *port-id*]

【config-mode】

Any

【parameter】

port-id: port number,string format: device number/slot number/port numbe,such as 0/0/1.

【description】

show cpu-statistics used to view the CPU statistics.

show cpu-statistics ethernet port-id command is used to view statistics of incoming CPU packets from a specified port.

【example】

View the CPU statistics of port 0/0/6

switch(config)#show cpu-statistics ethernet 0/0/46

Port number : e0/0/46

Input : 2668641 packets, 0 drops, 44092 bpdu

2263907 broadcasts, 404714 multicasts, 20 unicasts

1779741 64Bytes, 359075 128Bytes, 127595 256Bytes

153434 512Bytes, 248044 1024Bytes, 752 2048Bytes, 0 2048Bytes Over

8.2.8 clear cpu-statistics

【command】

clear cpu-statistics [ethernet *port-id*]

【config-mode】

Any

【parameter】

port-id: port number,string format: device number/slot number/port numbe,such as 0/0/1.

【description】

clear cpu-statistics used to clear the CPU statistics.

【example】

 # Clear the CPU statistics

switch#configure terminal

switch(config)#clear cpu-statistics

8.2.9 show utilization eth-trunk

【command】

show utilization eth-trunk

【config-mode】

Any

【parameter】

None

【description】

show utilization eth-trunk command is used to view the usage of the aggregation interface.

In the display information, press 0 to clear statistics, press U to roll back to the previous page, press D to display the next page, and press Enter to exit the view.

【example】

View the usage of the aggregation interface

switch(config)#show utilization eth-trunk

Link Utilization Averages Fri Feb 2 07:59:35 1970

Channel Receive Peak Rx Transmit Peak Tx

group pkts/sec pkts/sec pkts/sec pkts/sec

==========

1 0 0 0 0

=====spacebar->toggle screen U->page up D->page down CR->exit=====

8.2.10 show utilization interface

【command】

show utilization interface

【config-mode】

Any

【parameter】

None

【description】

show utilization interface command is used to view the real-time utilization of all ports

【example】

View the real-time utilization of all ports

switch(config-if-eth-trunk-2)#show utilization interface

Link Utilization Averages Fri Feb 2 08:10:28 1970

port link Receive Peak Rx Transmit Peak Tx

Status pkts/sec pkts/sec pkts/sec pkts/sec

==========

e0/0/1	down	0	0	0	0
e0/0/2	down	0	0	0	0
e0/0/3	down	0	0	0	0
e0/0/4	down	0	0	0	0
e0/0/5	down	0	0	0	0
e0/0/6	down	0	0	0	0
e0/0/7	down	0	0	0	0
e0/0/8	down	0	0	0	0
e0/0/9	down	0	0	0	0
e0/0/10	down	0	0	0	0
e0/0/11	down	0	0	0	0
e0/0/12	down	0	0	0	0
e0/0/13	down	0	0	0	0
e0/0/14	down	0	0	0	0
e0/0/15	down	0	0	0	0
e0/0/16	down	0	0	0	0
e0/0/17	down	0	0	0	0

=====spacebar->toggle screen U->page up D->page down CR->exit=====

8.2.11 show cpu-utilization

【command】

show cpu-utilization

【config-mode】

Any

【parameter】

None

【description】

show cpu-utilization command is used to view the CPU utilization information.

【example】

#View the CPU utilization information

switch#configure terminal

switch(config)#show cpu-utilization

CPU Information:

CPU Idle : 95 %

8.2.12 show flow-control interface

【command】

show flow-control interface [**ethernet** *port-id*]

【config-mode】

Any

【parameter】

port-id: port number,string format: device number/slot number/port numbe,such as 0/0/1.

【description】

show flow-control interface command is used to view flow control status information of all ports

show flow-control interface ethernet *port-id* command is used to view flow control status information for the specified port.

【example】

View flow control status information of all ports

switch(config)#show flow-control interface

Port Flow-Control-State

e0/0/1 enable

e0/0/2 disable

e0/0/3 disable

e0/0/4 disable

e0/0/5 disable

e0/0/6 disable

……

Parameter descriptions of show flow-control interface

Parameter	Description
Port	Port number
Flow-Control-State	Flow control enabled state

8.2.13 show mtu interface

【command】

show mtu interface [**ethernet** *port-id*]

【config-mode】

Any

【parameter】

port-id: port number,string format: device number/slot number/port number,such as 0/0/1

【description】

show mtu interface command is used to view the port mtu value.

【example】

View the mtu value of the port.

switch#show mtu interface

Port : Mtu

e0/0/1 : 12288

e0/0/2 : 12288

e0/0/3 : 12288

e0/0/4 : 12288

e0/0/5 : 12288

e0/0/6 : 12288

……

Parameter descriptions of show mtu interface

Parameter	Description
Port	port number
Mtu	mtu value of the port

8.2.14 show interface sfp

【command】

show interface sfp [**ethernet** *port-id*]

【config-mode】

Any

【parameter】

port-id: port number,string format: device number/slot number/port numbe,such as 0/0/1

【description】

show interface sfp command is used to view DDM information of the port.

If the port is not fiber port, there will be an error message.

If the port is not connected to the SFP optical module, there will be an error messag.

If the fiber port hardware does not support DDM, there will be an error message.

【example】

Show the DDM information for port 0/1/1.

switch#(config)#show interface sfp

Port e0/1/1 :

Common information:

Transceiver Type :SFP/SFP+

Compliance :10G BASE-SR

Connector Type :LC

WaveLength(nm) :850

Transfer Distance(m) :300(50um)

Digital Diagnostic Monitoring :YES

Manufacture information:

Manu. Serial Number :FIB2007211058

Manufacturing Date :2020-07-22

VendorName :OEM

Diagnostic information:

Temperature(℃) :24

Voltage(V) :3.37

Bias Current(mA) :6.53

Bias High Threshold(mA) :12.00

Bias Low Threshold(mA) :2.00

RX Power(dBM) :-40.00(Warning: exceed low threshold)

RX Power High Threshold(dBM) :-1.00

RX Power Low Threshold(dBM) :-11.10

TX Power(dBM) :-2.31

TX Power High Threshold(dBM) :-1.00

TX Power Low Threshold(dBM) :-7.30

Chapter 9 VLAN Interface

9.1 VLAN Interface Configure Commands

9.1.1 interface vlan-interface

【command】

interface vlan-interface *vlan-id*

no interface vlan-interface *vlan-id*

【config-mode】

Except System mode and Privilege EXEC mode

【parameter】

vlan-id: vlan id， integer form, the value ranges from 1-4094.

【description】

interface vlan-interface *vlan-id* command is used to create a VLAN interface and enter the vlan interface configure mode.

no interface vlan-interface *vlan-id* command is used to delete a vlan interface.

When the VLAN interface does not exist, the VLAN interface will be created and enter the VLAN interface configure mode at the same time; When the VLAN interface is present, only enter the VLAN interface configure mode.

【example】

#Create vlan interface 1.

switch#configure terminal

switch(config)#interface vlan-interface 1

switch(config-if-vlanInterface-1)#

9.1.2 description

【command】

description *description*

no description

【config-mode】

VLAN interface configure mode

【parameter】

description: interface description, maximum support 128 characters, Can't contain characters?.

【description】

description *description* command is used to configure VLAN interface description information.

no description command is used to restore the default configuration.

By default there is no description of configuration information.

【example】

Set the description of VLAN interface 1 to abc.

switch#configure terminal

switch(config)#interface vlan-interface 1

switch(config-if-vlanInterface-1)#description abc

9.1.3 ip address

【command】

ip address *ip-address ip-mask* [**override**]

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

【config-mode】

VLAN interface configure mode

【parameter】

ip-address: IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2.

ip-mask: decimal, format: x.x.x.x.such as 255.255.255.0

override: Directly override the existing IP, without it means config a new ip address.

【description】

ip address *ip-address ip-mask* command is used to config a ip address.

no ip address command is used to delete the ip address.

no ip address *ip-address ip-mask* command is used to delete a specified ip address.

A VLAN interface can be configured with a maximum of 32 IP addresses.

【example】

Configure the IP address 192.168.2.1/24 for VLAN interface 2

switch(config)#interface vlan-interface 2

switch(config-if-vlanInterface-2)#ip address 192.168.2.1 255.255.255.0

switch(config-if-vlanInterface-2)#

9.1.4 ip address primary

【command】

ip address primary *ip-address*

【config-mode】

VLAN interface config mode

【parameter】

ip-address: IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2.

【description】

ip address primary *ip-address* command is used to set the new primary IP address.

By default, the first configured IP address is the interface primary IP,but you can use this command to switch a new primary ip address

The input ip-address must be configured, otherwise the configuration will fail.

【example】

Configure the primary IP for VLAN interface 2.

switch(config-if-vlanInterface-2)#exit

switch(config)#interface vlan-interface 2

switch(config-if-vlanInterface-2)#ip address primary 1.1.1.1

9.1.5 ip address { dhcp | bootp }

【command】

ip address { dhcp | bootp }

no ip address { dhcp | bootp }

【config-mode】

VLAN interface configure mode

【parameter】

dhcp: Set the interface as a dhcp client .

bootp: Set the interface as a bootp client .

【description】

ip address{ dhcp | bootp } command is used to enable dhcp/bootp client.

no ip address{ dhcp | bootp } command is used to disable dhcp/bootp client .

The static IP must be removed before enable the dhcp/bootp cleint.

Dhcp/bootp clients can be configured on only one interface .

【example】

Enable dhcp client at VLAN interface 2

switch(config)#interface vlan-interface 2

switch(config-if-vlanInterface-2)#ip address dhcp

switch(config-if-vlanInterface-2)#

9.1.6 ip address range

【command】

ip address range *start-ip-address end-ip-address*

no ip address range [*start-ip-address end-ip-address*]

【config-mode】

VLAN interface configure mode

【parameter】

start-ip-address: Start IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2.

end-ip-address: End IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.20.

【description】

ip address range command is used to configure the range of ip address allowed for communication.

no ip address range command is used to restore the default configuration.

After configuring this command, only the IP within the range can communicate.

By default, all ip address can communicate.

【example】

Configure VLAN interface 1 to allow only users 192.168.11.102-192.168.11.200.

switch #configure terminal

switch(config)#interface vlan-interface 1

switch(config-if-vlanInterface-1)#ip address 192.168.11.101 255.255.0.0

switch(config-if-vlanInterface-1)#ip address range 192.168.11.102 192.168.11.200

9.1.7 ipv6 address { ipv6-address/M | autoconfig }

【command】

ipv6 address { *ipv6-address/M* | **autoconfig** }

no ipv6 address { *ipv6-address/M* | **autoconfig** }

【config-mode】

VLAN interface configure mode

【parameter】

ipv6-address: Global ipv6 address, hexadecimal format,such as 2003::100 .

M: IPv6 address prefix lengt, integer form, ranges from 1 to 64.

autoconfig: Enable stateless auto-configuration address.

【description】

ipv6 address *ipv6-address/M* command is used to config a static ipv6 address.

ipv6 address autoconfig command is used to enable stateless auto-configuration address.

no ipv6 address *ipv6-address/M* command is used to delete a static ipv6 address.

no ipv6 address autoconfig command is used to disable stateless auto-configuration address

【example】

Configure VLAN interface 1 Global unicast address 2003::1/64

switch(config)#interface vlan-interface 1

switch(config-if-vlanInterface-1)#ipv6 address 2003::1/64

9.1.8 ipv6 address { ipv6-address | auto } link-local

【command】

ipv6 address { *ipv6-address* | **auto** } **link-local**

no ipv6 address { *ipv6-address* | **auto** } **link-local**

【config-mode】

VLAN interface configure mode

【parameter】

ipv6-address: Ipv6 link-local address ,must begin with fe80.

auto: Enable automatically config the link-local address .

【description】

ipv6 address *ipv6-address* **link-local** command is used to configure the static link local address.

ipv6 address auto link-local command is used to enable automatically config the link-local address.

no ipv6 address *ipv6-address* **link-local** command is used to delete the static link local address.

no ipv6 address auto link-local command is used to disable automatically config the link-local address.

【example】

Enable VLAN interface 1 to configure the link local address automatically

switch(config)#interface vlan-interface 1

switch(config-if-vlanInterface-1)#ipv6 address auto link-local

9.1.9 ipv6 address ipv6-prefix eui-64

【command】

ipv6 address *ipv6-prefix/M* **eui-64**

no ipv6 address *ipv6-prefix/M* **eui-64**

【config-mode】

VLAN interface configure mode

【parameter】

ipv6-prefix/M: ipv6 address prefix, such as 2000::/64.

【description】

ipv6 address *ipv6-prefix/M* **eui-64** command is used to configure the IPV6 address prefix and use the eui-64 format generated IPv6 address.

no ipv6 address *ipv6-prefix/M* **eui-64** command is used to delete the eui-64 format ipv6 address.

The VLAN interface automatically generates an address based on the configured prefix +eui-64 interface ID.

【example】

Configure vlan interface 1 eui-64 address prefix as 2001::/64

switch(config)#interface vlan-interface 1

switch(config-if-vlanInterface-1)#ipv6 address 2001::/64 eui-64

9.1.10 ipv6 pathmtu

【command】

ipv6 pathmtu *mtu-value*

no ipv6 pathmtu

【config-mode】

VLAN interface configure mode

【parameter】

mtu-value: Maximum Transmission Unit, range: 1280-1500, in bytes.

【description】

ipv6 pathmtu command is used to configure the interface path maximum transmission unit.

no ipv6 pathmtu command is used to restore the default configuration.

By default, pathmtu is 1500 bytes.

【example】

#Set the ipv6 pathmtu value of interface vlan 1 to 1360 bytes.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ipv6 pathmtu 1360

9.1.11 ipv6 nd dad attemps

【command】

ipv6 nd dad attemps *attemp-value*

no ipv6 nd dad attemps

【config-mode】

VLAN interface configure mode

【parameter】

attemp-value: DAD times , Range 0-20; default 1.

【description】

ipv6 nd dad attemps *attemp-value* command is used to configure duplicate address detection times.

no ipv6 nd dad attemps command is used to restore the default configuration.

By default, duplicate addresses are detected once.

If the value is set to 0, the duplicate address detection function is disabled.

【example】

Configure the duplicate address detection twice on VLAN1.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ipv6 nd dad attemps 2

9.1.12 bandwidth

【command】

bandwidth *bandwidth-value*

no bandwidth

【config-mode】

VLAN interface configure mode

【parameter】

bandwidth-value: Integer form, range 1-10000000, in kbs.

【description】

bandwidth command is used to set the VLAN interface bandwidth.

no bandwidth command is used to restore the default configuration.

Logical bandwidth is only used to calculate the cost of a VLAN interface in ospf.

【example】

Set the bandwidth of interface vlan 1 to 10000000kbs.

switch#configure terminal

switch(config)#interface vlan-interface 1

switch(config-if-vlanInterface-1)##bandwidth 10000000

9.1.13 shutdown

【command】

shutdown

no shutdown

【config-mode】

VLAN interface configure mode

【parameter】

None

【description】

shutdown command is used to disable the vlan interface .

no shutdown command is used to enable the vlan interace.

By default,vlan interface is enable.

After the interface is disabled, the interface status becomes unavailable; When the interface is enabled, the interface state won't immediately becomes available, but also according to other constraints.

【example】

#Disable or enable the interface vlan 1.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#shutdown

Switch(config-if-vlanInterface-1)#no shutdown

9.2 VLAN Interface Debug Commands

9.2.1 show ip interface vlan-interface

【command】

show ip interface vlan-interface *vlan-id*

【config-mode】

Any

【parameter】

vlan-id: vlan id, integer form, the value ranges from 1-4094.

【description】

show ip interface vlan-interface *vlan-id* command is used to view information about the vlan interface.

【example】

show information about interface vlan 1

switch(config)#show ip interface vlan-interface 1

Show information of interface

The mac-address of interface is 30:b9:b0:01:f2:f1

Interface name : VLAN-IF1

Primary ip address : 10.2.5.51/255.255.255.0

Secondary ip address : 192.168.2.22/255.255.255.0

VLAN : 1

Address-range : 2.2.2.2-2.2.20.2,

Interface status : Up

Total entries: 1 interface.

9.2.2 show ipv6 nd dad attemps

【command】

show ipv6 nd dad attemps

【config-mode】

Any

【parameter】

None

【description】

show ipv6 nd dad attemps command is used to view duplicate address detection configuration information.

【example】

#Show the settings about duplicate address detection

switch(config)#show ipv6 nd dad attemps

Neighbor dad attemps of interface:

Interface name : VLAN-IF1

Attemps : 1

Interface name : loopback0

Attemps : 1

Interface name : superVLAN-IF1

Attemps : 1

Total entries: 3 interface.

9.2.3 show ip dhcp lease

【command】

show ip dhcp lease

【config-mode】

Any

【parameter】

None

【description】

show ip dhcp lease command is used to view the dhcp lease information of interface.

【example】

#View the dhcp lease information of interface

switch(config)#show ip dhcp lease

DHCP is running on interface VLAN-IF2(sw1).

Obtained DHCP parameters:

IP Address : 0.0.0.0

IP Mask : 0.0.0.0

IP Gateway : 0.0.0.0

DHCP Server : 0.0.0.0

Lease Info : N/A

Lease Obtained: N/A

9.2.4 show ipv6 interface vlan-interface

【command】

show ipv6 interface vlan-interface *vlan-id*

【config-mode】

Any

【parameter】

vlan-id: VLAN ID list, integral form, the values range 1-4094.

【description】

show ipv6 interface vlan-interface *vlan-id* command is used to view the ipv6 address information of vlan interface.

【example】

View the ipv6 address information of vlan interface 1

switch(config)#show ipv6 interface vlan-interface 1
Ipv6 forwarding:disable

Ipv6 information of interface:

Interface name : VLAN-IF1
Ipv6 enabled : Enabled
Ipv6 ip address : 2003::10/64
Auto config : Disabled
Auto link-local : Disabled
Config link-local : None
Link-local address : fe80::30b9:b000:101:f2f1%sw0/64
Path MTU : 1500
Interface status : Up

Total entries: 1 interface.

Parameter descriptions of show ipv6 interface vlan-interface

Parameter	Description
Ipv6 forwarding	Status of Ipv6 forwarding
Interface name	Interface name

Parameter	Description
Ipv6 enabled	Status of IPV6
Ipv6 ip address	Ipv6 address
Auto config	Automatically generated IPV6 address
Config link-local	Manually configured link local address
Link-local address	link local address automatically
Path MTU	Path maximum transmission unit
Interface status	Interface status: up、down

Chapter 10 Supervlan Interface

10.1 Supervlan Interface Commands

10.1.1 interface supervlan-interface

【command】

interface supervlan-interface *id*

no interface supervlan-interface *id*

【config-mode】

Any mode except the system mode and Privilege EXEC mode

【parameter】

id: interface id, integer form,ranges from 1 to 128.

【description】

interface supervlan-interface *id* command is used to create a supervlan interface and enter the supervlan interface configure mode.

no interface supervlan-interface *id* used to delete supervlan interface.

When the supervlan interface does not exist, the supervlan interface will be created and enter the supervlan interface configure mode at the same time; When the supervlan interface is present, only enter the supervlan interface configure mode.

【example】

#Add an interface of supervlan 1.

switch#configure terminal

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)#

10.1.2 subvlan

【command】

subvlan *vlan-list*

no subvlan *vlan-list*

【config-mode】

supervlan interface configure mode

【parameter】

vlan-list: VLAN list. The VLAN ID ranges from 1 to 4094. The VLAN list can contain one or multiple VLAN ids . Discontinuous VLAN ids are separated by the symbol ", ";Consecutive VLAN ids are connected with the symbol "-",such as 8,9,11-15.

【description】

subvlan *vlan-list* command is used to config the subvlan that is added to the supervlan interface.

no subvlan *vlan-list* command is used to delete the subvlan.

By default,there are no subvlan in the supervlan interface; A maximum of 64 subvlans can be added to the supervlan.

【example】

#Set the subvlans as 3-20 and 30 to interface supervlan 1.

switch#configure terminal

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)#subvlan 3-20,30

switch(config-if-superVLANInterface-1)#

10.1.3 description

【command】

description *description*

no description

【config-mode】

supervlan interface configure mode

【parameter】

description: interface description, maximum support 128 characters, Can't contain characters?.

【description】

description *description* command is used to configure supervlan interface description information.

no description command is used to restore the default configurations.

By default there is no description of configuration information.

【example】

Set the description of supervlan interface 1 to abc.

switch#configure terminal

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)#description abc

10.1.4 ip address

【command】

ip address *ip-address ip-mask* **[override]**

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

【config-mode】

supervlan interface configure mode

【parameter】

ip-address: IPv4 address, format: x.x.x.x ,such as 2.2.2.2.

ip-mask: format: x.x.x.x.such as 255.255.255.0

override: Directly override the existing IP, without it means config a new ip address.

【description】

ip address *ip-address ip-mask* command is used to config a ip address.

no ip address command is used to delete the ip address.

no ip address *ip-address ip-mask* command is used to delete a specified ip address.

A supervlan interface can be configured with a maximum of 32 IP addresses.

【example】

Configure the IP address 192.168.2.1/24 for supervlan interface 2

switch(config)#interface supervlan-interface 2

switch(config-if-superVLANInterface-2)#ip address 192.168.2.1 255.255.255.0

switch(config-if-superVLANInterface-2)#

10.1.5 ip address primary

【command】

ip address primary *ip-address*

【config-mode】

supervlan interface configure mode

【parameter】

ip-address: IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2

【description】

ip address primary *ip-address* command is used to set the new primary IP address.

By default, the first configured IP address is the interface primary IP,but you can use this command to switch a new primary ip address

The input ip-address must be configured, otherwise the configuration will fail.

【example】

Configure the primary IP for supervlan interface 2.

switch(config)#interface supervlan-interface 2

switch(config-if-superVLANInterface-2)#ip address primary 1.1.1.1

switch(config-if-superVLANInterface-2)#

10.1.6 ip address { dhcp | bootp }

【command】

ip address { dhcp | bootp }

no ip address { dhcp | bootp }

【config-mode】

supervlan interface configure mode

【parameter】

dhcp: Set the interface as a dhcp client .

bootp: Set the interface as a bootp client .

【description】

ip address{ dhcp | bootp } command is used to enable dhcp/bootp client.

no ip address{ dhcp | bootp } command is used to disable dhcp/bootp client .

The static IP must be removed before enable the dhcp/bootp cleint.

Dhcp/bootp clients can be configured on only one interface .

【example】

Enable dhcp client at supervlan interface 2

switch(config)#interface supervlan-interface 2

switch(config-if-superVLANInterface-2)#ip address dhcp

switch(config-if-superVLANInterface-2)#

10.1.7 ip address range

【command】

ip address range *start-ip-address end-ip-address*

no ip address range [*start-ip-address end-ip-address* **]**

【config-mode】

supervlan interface configure mode

【parameter】

start-ip-address: Start IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2.

end-ip-address: End IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.20.

【description】

ip address range command is used to configure the range of ip address allowed for communication.

no ip address range command is used to restore the default configuration.

After configuring this command, only the IP within the range can communicate.

By default, all ip address can communicate .

【example】

Configure VLAN interface 1 to allow IP 192.168.11.102-192.168.11.200.

switch#configure terminal

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)#ip address 192.168.11.101 255.255.0.0

switch(config-if-superVLANInterface-1)#ip address range 192.168.11.102 192.168.11.200

10.1.8 ipv6 address { ipv6-address/M | autoconfig }

【command】

ipv6 address { *ipv6-address/M* | **autoconfig** }

no ipv6 address { *ipv6-address/M* | **autoconfig** }

【config-mode】

supervlan interface configure mode

【parameter】

ipv6-address: Global ipv6 address, hexadecimal format,such as 2003::100 .

M: IPv6 address prefix lengt， integer form, ranges from 1 to 64.

autoconfig: Enable stateless auto-configuration address.

【description】

ipv6 address *ipv6-address/M* command is used to config a static ipv6 address.

ipv6 address autoconfig command is used to enable stateless auto-configuration address.

no ipv6 address *ipv6-address/M* command is used to delete a static ipv6 address.

no ipv6 address autoconfig command is used to disable stateless auto-configuration address.

【example】

Configure the ipv6 address of supervlan interface 1 as 2003::1/64

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)#ipv6 address 2003::1/64

10.1.9 ipv6 address { ipv6-address | auto } link-local

【command】

ipv6 address { *ipv6-address* | **auto** } **link-local**

no ipv6 address { *ipv6-address* | **auto** } **link-local**

【config-mode】

supervlan interface configure mode

【parameter】

ipv6-address: Ipv6 link-local address ,must begin with fe80.

auto: Enable automatically config the link-local address.

【description】

ipv6 address *ipv6-address* **link-local** command is used to configure the static link local address.

ipv6 address auto link-local command is enable automatically config the link-local address.

no ipv6 address *ipv6-address* **link-local** command is used to delete the static link local address.

no ipv6 address auto link-local command is used to disable automatically config the link-local address.

【example】

Enable supervlan interface 1 to configure the link local address automatically

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)#ipv6 address auto link-local

10.1.10 ipv6 address ipv6-prefix eui-64

【command】

ipv6 address *ipv6-prefix/M* **eui-64**

no ipv6 address *ipv6-prefix/M* **eui-64**

【config-mode】

supervlan interface configure mode

【parameter】

ipv6-prefix/M: ipv6 address prefix， such as 2000::/64

【description】

ipv6 address *ipv6-prefix/M* **eui-64** command is used to configure the IPv6 address prefix and use the eui-64 format generated IPV6 address.

no ipv6 address *ipv6-prefix/M* **eui-64** command is used to delete the eui-64 format ipv6 address..

The supervlan interface automatically generates an address based on the configured prefix +eui-64 interface ID.

【example】

Configure supervlan interface 1 eui-64 address prefix as 2001::/64

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)#ipv6 address 2001::/64 eui-64

10.1.11 ipv6 pathmtu

【command】

ipv6 pathmtu *mtu-value*

no ipv6 pathmtu

【config-mode】

Supervlan interface configure mode

【parameter】

mtu-value: Maximum Transmission Unit, range: 1280-1500, in bytes

【description】

ipv6 pathmtu command is used to configure the interface path maximum transmission unit.

no ipv6 pathmtu command is used to restore the default configuration.

By default, pathmtu is 1500 bytes.

【example】

#Set the ipv6 pathmtu value of supervlan interface 1 to 1360 bytes.

Switch#configure terminal

Switch(config)#interface supervlan-interface 1

Switch(config-if-superVLANInterface-1)#ipv6 pathmtu 1360

10.1.12 ipv6 nd dad attemps

【command】

ipv6 nd dad attemps *attemp-value*

no ipv6 nd dad attemps

【config-mode】

Supervlan interface configure mode

【parameter】

attemp-value: DAD times , range 0-20; default 1.

【description】

ipv6 nd dad attemps *attemp-value* command is used to configure duplicate address detection times.

no ipv6 nd dad attemps command is used to restore the default configuration.

By default, duplicate addresses are detected once.

If the value is set to 0, the duplicate address detection function is disabled.

【example】

Configure the duplicate address detection twice on supervlan interface 1.

Switch#configure terminal

Switch(config)#interface supervlan-interface 1

Switch(config-if-superVLANInterface-1)#ipv6 nd dad attemps 2

10.1.13 bandwidth

【command】

bandwidth *bandwidth-value*

no bandwidth

【config-mode】

supervlan interface configure mode

【parameter】

bandwidth-value: Integer form, range 1-10000000, in kbs.

【description】

bandwidth command is used to set the VLAN interface bandwidth.

no bandwidth command is used to restore the default configuration.

Logical bandwidth is only used to calculate the cost of a supervlan interface in ospf.

【example】

Set the bandwidth of supervlan interface 1 to 10000000kbs.

switch#configure terminal

switch(config)#interface supervlan-interface 1

switch(config-if-superVLANInterface-1)##bandwidth 10000000

10.1.14 shutdown

【command】

shutdown

no shutdown

【config-mode】

supervlan interface configure mode

【parameter】

None

【description】

shutdown command is used to disable the vlan interface.

no shutdown command is used to enable the vlan interace.

By default,vlan interface is enable.

After the interface is disabled, the interface status becomes unavailable; When the interface is enabled, the interface state won't immediately becomes available, but also according to other constraints

【example】

Disable or enable the interface vlan 1.

Switch(config)#interface supervlan-interface 1

Switch(config-if-superVLANInterface-1)#shutdown

Switch(config-if-superVLANInterface-1)#no shutdown

10.2 Supervlan Interface Debug Commands

10.2.1 show ip interface supervlan-interface

【command】

show ip interface supervlan-interface *id*

【config-mode】

Any

【parameter】

id: supervlan id, integer form, the value ranges from 1-128.

【description】

show ip interface supervlan-interface *id* used to view information about the supervlan interface.

【example】

View information about the supervlan interface 1

switch(config)#show ip interface supervlan-interface 1

Show information of interface

The mac-address of interface is 30:b9:b0:01:f2:f1

Interface description : abc

Interface name : superVLAN-IF1

Primary ip address : 10.1.1.1/255.255.255.0

Secondary ip address : 10.2.1.1/255.255.255.0

VLAN : 3-20,30

Address-range : 10.0.0.0-255.0.0.0,

Interface status : Down

Total entries: 1 interface.

10.2.2 show ipv6 nd dad attemps

【command】

show ipv6 nd dad attemps

【config-mode】

Any

【parameter】

None

【description】

show ipv6 nd dad attemps used to view duplicate address detection configuration information.

【example】

View duplicate address detection configuration information

switch(config)#show ipv6 nd dad attemps

Neighbor dad attemps of interface:

Interface name : VLAN-IF1

Attemps : 1

Interface name : loopback0

Attemps : 1

Interface name : superVLAN-IF1

Attemps : 1

Total entries: 3 interface.

10.2.3 show ip dhcp lease

【command】

show ip dhcp lease

【config-mode】

Any

【parameter】

None

【description】

show ip dhcp lease used to view the dhcp lease information of interface.

【example】

View the dhcp lease information of interface

switch(config)#show ip dhcp lease

DHCP is running on interface superVLAN-IF-IF2(sw2).

Obtained DHCP parameters:

IP Address : 0.0.0.0

IP Mask : 0.0.0.0

IP Gateway : 0.0.0.0

DHCP Server : 0.0.0.0

Lease Info : N/A

Lease Obtained: N/A

Parameter descriptions of show ip dhcp lease

Parameter	Description

Parameter	Description
IP Address	IP Address
IP Mask	IP Mask
IP Gateway	IP Gateway
DHCP Server	DHCP Server
Lease Info	Remaining lease term
Lease Obtained	The last time for lease time

10.2.4 show ipv6 interface supervlan-interface

【command】

show ipv6 interface supervlan-interface *id*

【config-mode】

Any

【parameter】

id: interface id, integer form,ranges from 1 to 128.

【description】

show ipv6 interface supervlan-interface *id* command is used to view the ipv6 address information of vlan interface.

【example】

View the ipv6 address information of supervlan interface 1

switch(config-if-vlanInterface-1)# show ipv6 interface supervlan-interface 1

The mac-address of interface is 30:b9:b0:01:f2:f1

Ipv6 forwarding:disable

Ipv6 information of interface:

Interface description : abc

Interface name : superVLAN-IF1

Ipv6 enabled : Enabled

Ipv6 ip address : 2013::/64

: 2014::32b9:b0ff:fe01:f2f1/64

: 2015::10/64

Auto config : Enabled

Auto link-local : Enabled

Config link-local : fe80::2001

Link-local address : None

Path MTU : 1500

Interface status : Down

Total entries: 1 interface.

Parameter descriptions of show ipv6 interface

Parameter	Description

Parameter	Description
Ipv6 forwarding	Status of Ipv6 forwarding
Interface name	Interface name
Ipv6 enabled	Status of IPV6
Ipv6 ip address	Ipv6 address
Auto config	Automatically generated IPV6 address
Config link-local	Manually configured link local address
Link-local address	link local address automatically
Path MTU	Path maximum transmission unit
Interface status	Interface status: up、down

Chapter 11 Loopback Interface

11.1 Loopback Interface Configure Commands

11.1.1 interface loopback-interface

【command】

interface loopback-interface *id*

no interface loopback-interface *id*

【config-mode】

Global configuration mode

【parameter】

id: loopback interface id,range from 0 to 1.

【description】

interface loopback-interface command is used to create a loopback interface and enter the loopback interface configure mode.

no interface loopback command is used to delete loopback interface.

By default,there is no loopback interface; When the loopback interface does not exist, it will be created and enter the loopback interface configure mode at the same time; When the loopback interface is present, only enter the loopback interface configure mode.

【example】

Create loopback interface 1

switch#configure terminal

switch(config)#interface loopback-interface 1

switch(config-if-loopBackInterface-1)#

11.1.2 ip address

【command】

ip address *ip-address ip-mask*

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

【config-mode】

loopback interface configure mode

【parameter】

ip-address: IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2.

ip-mask: decimal, format: x.x.x.x.such as 255.255.255.0.

【description】

ip address *ip-address ip-mask* command is used to config a ip address.

no ip address command is used to delete the ip address.

no ip address *ip-address ip-mask* command is used to delete a specified ip address.

A loopback interface can be configured with a maximum of 32 IP addresses.

【example】

Configure the IP address 192.168.2.1/24 for loopback interface 2

switch(config)#interface loopback-interface 1

switch(config-if-loopBackInterface-1)#ip address 1.1.1.1 255.255.255.0

switch(config-if-loopBackInterface-1)#

11.1.3 ip address primary

【command】

ip address primary *ip-address*

【config-mode】

loopback interface configure mode

【parameter】

ip-address: IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2.

【description】

ip address primary *ip-address* command is used to set the new primary IP address.

By default, the first configured IP address is the interface primary IP,but you can use this command to switch a new primary ip address

The input ip-address must be configured, otherwise the configuration will fail.

【example】

Configure the primary IP for loopback interface 1.

switch(config)#interface loopback-interface 1

switch(config-if-loopBackInterface-1)#ip address primary 1.1.1.1

switch(config-if-loopBackInterface-1)#

11.2 Loopback Interface Debug Commands

11.2.1 show ip interface loopback-interface

【command】

show ip interface loopback-interface *id*

【config-mode】

Any

【parameter】

id: loopback interface id,range from 0 to 1.

【description】

show ip interface loopback-interface *id* command is used to view information about the loopback interface.

【example】

View information about the loopback interface 1.

switch(config)#show ip interface loopback-interface 1

Show information of interface

The mac-address of interface is 44:18:47:00:00:00

Interface name : loopback1

Primary ipaddress : 2.2.2.2/255.255.255.0

Secondary ipaddress : 1.1.1.1/255.255.255.0

Interface status : Up

Total entries: 1 interface.

11.2.2 show ipv6 interface loopback-interface

【command】

show ipv6 interface loopback-interface ***id***

【config-mode】

Any

【parameter】

id : loopback interface id,range from 0 to 1

【description】

show ipv6 interface loopback-interface *id* command is used to view ipv6 address information about the loopback interface.

【example】

View the ipv6 address information of loopback interface 1

switch(config)#show ipv6 interface loopback-interface 1

Ipv6 forwarding:disable

Ipv6 informations of interface:

Interface name : loopback1

Ipv6 enabled : Enabled

Ipv6 ipaddress : 2003::10/64

Auto config : Disabled

Auto link-local : Disabled

Config link-local : None

Link-local address : fe80::4418:4700:200:0%sw1/64

Path MTU : 1500

Interface status : Up

Total entries: 1 interface.

Chapter 12 Internal Interface

12.1 Internal Interface Configuration Commands

12.1.1 interface internal-interface

【command】

interface internal-interface *id*

no interface internal-interface *id*

【config-mode】

Global configuration mode

【parameter】

id: Internal interface id ,value is 0.

【description】

interface internal-interface command is used to create administrative interfaces and enter configuration mode.

no interface internal-interface command is used to delete the internal-interface.

The internal-interface is only used for upgrade software. By default, there is no internal-interface.

By default,there is no internal-interface; When the internal-interface does not exist, it will be created and enter the internal-interface configure mode at the same time; When the internal-interface is present, only enter the internal-interface configure mode.

【example】

Create loopback interface 0

switch#configure terminal
switch(config)#interface internal-interface 0

switch(config-if-internalInterface-0)#

12.1.2 ip address

【command】

ip address *ip-address ip-mask*

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

【config-mode】

Internal interface configure mode

【parameter】

ip-address: IPv4 address, decimal, format: x.x.x.x ,such as 2.2.2.2.

ip-mask: decimal, format: x.x.x.x.such as 255.255.255.0.

【description】

ip address *ip-address ip-mask* command is used to config a ip address.

no ip address command is used to delete the ip address.

no ip address *ip-address ip-mask* command is used to delete a specified ip address.

A internal-interface interface can be configured with a maximum of 32 IP addresses..

By default,there is no internal-interface; When the internal-interface does not exist, it will be created and enter the internal-interface configure mode at the same time; When the internal-interface is present, only enter the internal-interface configure mode.

【example】

Create internal-interface interface 0 and add ipv4 address as 1.1.1.1/24

switch#configure terminal

switch(config)#interface internal-interface 0

switch(config-if-internalInterface-0)#ip add 1.1.1.1 255.255.255.0

12.2 Management Interface Debug Commands

12.2.1 show ip interface internal-interface

【command】

show ip interface internal-interface *id*

【config-mode】

Any

【parameter】

id: management interface id ,value is 0.

【description】

show ip interface internal-interface *id* command is used to view the information about management interface.

【example】

View the information about management interface

switch(config-if-internalInterface-0)#show ip interface internal-interface 0

Show information of interface
The mac-address of interface is 44:18:47:00:00:00
Interface name : internal0
Primary ipaddress : 3.3.3.3/255.255.255.0
Secondary ipaddress : None
Mac-address : 00:e0:4c:00:00:00
Interface status : Up

Total entries: 1 interface.

Chapter 13 LACP

13.1 LACP configuration the commands

13.1.1 interface eth-trunk

【the command】

interface eth-trunk *eth-trunk-id*

no interface eth-trunk *eth-trunk-id*

【config-mode】

Global configuration mode

【parameter】

eth-trunk-id: Link aggregation group ID,The value ranges from 1 to 16.

【description】

interface eth-trunk *eth-trunk-id* the command is used to create a link aggregation group and enter the aggregation configuration mode.

no interface eth-trunk *eth-trunk-id* the command is used to delete a link aggregation group.

By default, no link aggregation group is created

【example】

#Create link aggregation group 1.

Switch#configure terminal

Switch(config)#interface eth-trunk 1

13.1.2 link-aggregation mode

【the command】

link-aggregation mode {dynamic | static}

no link-aggregation mode

【config-mode】

Aggregation group configuration mode

【parameter】

Dynamic: Indicates dynamic aggregation group.

static: Indicates static aggregation group.

【description】

link-aggregation mode the command is used to configure the link aggregation group mode.

no link-aggregation mode the command is used to restore the default situation.

By default, the default is a static aggregation group.

【example】

#Create a dynamic link aggregation group with link aggregation group number 1.

Switch#configure terminal

Switch(config)#interface eth-trunk 1

Switch(config-if-eth-trunk-1)#link-aggregation mode dynamic

13.1.3 link-aggregation members

【the command】

link-aggregation members ethernet *port-id*

no link-aggregation members ethernet *port-id*

【config-mode】

Link aggregation group configuration mode

【parameter】

port-id: Port number, In the format of device number/slot number/port number, for example, 0/0/1.

【description】

link-aggregation members ethernet the command is used to add a member port to a link aggregation group.

no link-aggregation members ethernet the command is used to delete a member port from a link aggregation group.

By default, a link aggregation group has no member.

Note:

1. Link aggregation groups support up to eight ports to join.

2. After a port has been added to a link aggregation group port, it cannot be added to another link aggregation group.

3. When multiple member ports are added to a link aggregation group at the same time, the link types of the member ports need to be the same.

【example】

#Add member port 0/0/1 for link aggregation group 1.

Switch#configure terminal

Switch(config)#interface eth-trunk 1

Switch(config-if-eth-trunk-1)#link-aggregation members ethernet 0/0/1

13.1.4 link-aggregation eth-trunk

【the command】

link-aggregation eth-trunk *eth-trunk-id*

no link-aggregation eth-trunk

【config-mode】

Port configuration mode

【parameter】

eth-trunk-id: Link aggregation group number, the value range is 1-16.

【description】

link-aggregation eth-trunk *eth-trunk-id* the command is used to configure a port to join an link aggregation group.

no link-aggregation eth-trunk the command is used to configure a port to leave the link aggregation group.

By default, the port does not join any aggregation group.

Note:

Before the port joins the link aggregation group, you need to determine whether the link aggregation group has been created, if it has not been created, the port cannot join the aggregation group.

【example】

#Configure port 0/0/1 to join link aggregation group 1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)##link-aggregation eth-trunk 1

13.1.5 lacp mode

【the command】

lacp mode {active | passive}

no lacp mode

【config-mode】

Port configuration mode

【parameter】

active: Indicates that the port joins the specified link aggregation group in an active form.

passive: Indicates that the port joins the specified link aggregation group in a passive form.

【description】

lacp mode the command is used to configure the port negotiation mode.

no lacp mode the command is used to restore the default situation.

By default, the default is active negotiation mode.

【example】

#Configure port 0/0/1 to be in active negotiation mode.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#lacp mode active

13.1.6 lacp period

【the command】

lacp period {long | short}

【config-mode】

Port configuration mode

【parameter】

long: Indicates slow mode, where the device sends LACP messages with a period of 30 seconds and a timeout of 90 seconds.

short: Indicates fast mode, where the device sends LACP messages with a period of 1 second and a timeout of 3 seconds.

【description】

lacp period the command is used to configure the port LACP timeout mode.

By default, the default is long mode.

【example】

#Configure port 0/0/1 to slow mode.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#lacp period short

13.1.7 lacp port-priority

【the command】

lacp port-priority *value*

no lacp port-priority

【config-mode】

Port configuration mode

【parameter】

value: This parameter is used to set the LACP priority of a port, the value range is 1-65535, the default value is 128.

【description】

lacp port-priority the command is used to set the LACP priority of a port.

no lacp port-priority the command is used to restore the default situation.

By default, the port LACP priority is 128.

The smaller the LACP priority of the port, then the higher the priority level.

【example】

#Configure the LACP priority of port 0/0/1 to 2000.

Switch#configure terminal

Switch(config)#interface eth 0/0/1

Switch(config-if-ethernet-0/0/1)#lacp port-priority 2000

13.1.8 lacp system-priority

【the command】

lacp system-priority *value*

no lacp system-priority

【config-mode】

Global configuration mode

【parameter】

value: This parameter is used to Configure the system LACP priority, the value range is 1-65535, the default value is 32768.

【description】

lacp system-priority the command is used to set the system LACP priority.

no lacp system-priority the command is used to restore the system LACP priority default value.

By default, system LACP priority is 32768.

The smaller the system LACP priority value , then the higher the priority level.

【example】

#Configure the system's LACP priority to 2000.

Switch#configure terminal

Switch(config)#lacp system-priority 1000

13.1.9 link-aggregation load-balance

【the command】

link-aggregation load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no link-aggregation load-balance

【config-mode】

Global configuration mode

【parameter】

dst-ip: Destination ip address based load balancing policy.

dst-mac: Destination mac address based load balancing policy.

src-dst-ip: Based on the source ip address or destination ip address load balancing policy, the source ip address and destination ip address of the traffic can be changed at the same time or one of them can be changed separately.

src-dst-mac: Based on the source mac address or destination mac address load balancing policy, the source mac address and destination mac address of the traffic can be changed at the same time or one of them can be changed separately.

src-ip: Source ip address based load balancing policy.

src-mac: Source mac address based load balancing policy.

【description】

link-aggregation load-balance the command is used to configure the load balancing policy for the aggregation group.

no link-aggregation load-balance the command is used to restore the default situation.

By default, the load balancing policy is src-mac.

【example】

#Configure the load balancing policy src-mac.

Switch#configure terminal

Switch(config)#link-aggregation load-balance src-mac

13.2 Link aggregation monitoring and debugging the commands

13.2.1 show lacp local

【the command】

show lacp local

【config-mode】

Arbitrary the command mode

【parameter】

None

【description】

show lacp local the command is used to display local LACP information.

【example】

#display local LACP information.

Switch#configure terminal

Switch(config)#show lacp local

Load balance: src-mac

eth-trunk ID: 1, dynamic channel

Port State A-Key O-Key Priority Logic-port Actor-state

e0/0/2	bndl	2	2	128	2	10111100
e0/0/4	bndl	2	2	128	2	10111100

actor-state: activity/timeout/aggregation/synchronization

collecting/distributing/defaulted/expired

show lacp local display field description.

Field	Description
Port	Port number
State	LACP Member Status
A-Key	Management Key, fixed as link aggregation group id+1.
O-Key	Operation Key, O-Key the same port in order to converge together, the value is the same as the value of A-Key.
Priority	Port LACP priority
Logic-port	Logical port number
Actor-state	The port status information is as follows: Activity：The master-slave status of the port in link control, 0 means Passive, 1 means Active. Timeout：Timeout time, 0 means long timeout, 1 means short timeout. Aggregation：TRUE(1) means the link is aggregatable, FALSE(0) means the link is independent link and not aggregatable. Synchronization：Indicates whether the current aggregation of the port is complete. TRUE(1) indicates that the sending link is in the IN_SYNC

state, that is, the interface has been assigned to the correct aggregation group, and FALSE(0) indicates that the link is in the OUT_OF_SYNC state, that is, the interface has not yet selected the correct aggregation group.

Collecting：TRUE(1) means the current link is packet-enable, otherwise it is FALSE(0).

Distributing：TRUE(1) means the current link is enabled to send packets, otherwise it is FALSE(0).

Defaulted：TRUE(1) means that the Partner information used by the Actor is from the default value configured by the administrator.FALSE(0) means that the Partner information used by the Actor is from the received LACPDU.

Expired：TRUE(1) means that the Actor RX state machine is in the timeout state, otherwise it is not in the timeout state.

13.2.2 show lacp neighbor

【the command】

show lacp neighbor [*eth-trunk id*]

【config-mode】

Arbitrary the command mode

【parameter】

eth-trunk id: Displays the specified LACP neighbor information.

【description】

show lacp neighbor the command displays the LACP neighbor information.

If the eth-trunk id parameter is not specified, information about all LACP neighbors that have been created is displayed.

If the eth-trunk id parameter is specified, only this LACP neighbor information is displayed.

【example】

#View LACP neighbor information.

Switch#configure terminal

Switch(config)#show lacp neighbor

eth-trunk ID: 1

Local	Port	Key	Pri	ID	Timeout	Nei-state
e0/0/2	2	3	100	32768,00017a00041e	2(3)	10111100
e0/0/4	6	3	128	32768,00017a00041e	3(3)	10111100

nei-state: activity/timeout/aggregation/synchronization

collecting/distributing/defaulted/expired

show lacp neighbor display field description.

Field	Description
Local	Local port number
Port	Neighbor Port Number
Key	Neighborhood Management Key, fixed as link aggregation group id+1
Pri	Neighbor port LACP priority
ID	Neighborhood system LACP priority information
Timeout	Port LACP timeout mode: long：In slow mode, the device sends LACP messages with a period of 30 seconds and a timeout of 90 seconds. short： In fast mode, the device sends LACP messages with a period of 1 second and a timeout of 3 seconds.

Nei-state	The neighbor port status information is as follows: Activity：The master-slave status of the port in link control, 0 means Passive, 1 means Active. Timeout：Timeout time, 0 means long timeout, 1 means short timeout. Aggregation：Indicates the aggregation capability of the port.TRUE(1) means the link is aggregatable, FALSE(0) means the link is a separate link and not aggregatable. Synchronization：Indicates whether the current aggregation of the port is complete. TRUE(1) indicates that the sending link is in the IN_SYNC state, i.e., the port has been assigned to the correct aggregation group, and FALSE(0) indicates that the link is in the OUT_OF_SYNC state, i.e., the port has not yet selected the correct aggregation group. Collecting：TRUE(1) means the current link is packet-enable, otherwise it is FALSE(0). Distributing：TRUE(1) means the current link is enabled to send packets, otherwise it is FALSE(0). Defaulted：TRUE(1) means that the Partner information used by the Actor is from the default value configured by the administrator.FALSE(0) means that the Partner information used by the Actor is from the received LACPDU. Expired：TRUE(1) means that the Actor RX state machine is in the timeout state, otherwise it is not in the timeout state.

13.2.3 show lacp sys-id

【the command】

show lacp sys-id

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show lacp sys-id the command displays the system LACP priority information.

【example】

#View system LACP priority information

Switch#configure terminal

Switch(config)#show lacp sys-id

13.2.4 debug lacp

【the command】

debug lacp

no debug lacp

【config-mode】

Global configuration mode

【parameter】

none

【description】

debug lacp the command is used to enables the lacp debugging function.

no debug lacp the command is used to disable the lacp debugging function.

【example】

#Enables the LACP debugging function.

Switch#configure terminal

Switch(config)#debug lacp

Chapter 14 Port Isolation

14.1 Port isolation configuration the commands

14.1.1 port-isolation uplink ethernet

【the command】

port-isolation uplink ethernet *port-id* **[[to] ethernet** *port-id* **]**

no port-isolation uplink { all | ethernet *port-id* **[[to] ethernet** *port-id* **] }**

【config-mode】

Port configuration mode

【parameter】

port-id: Port number in the format of device number/slot number/port number, e.g. 0/0/1.

to: Indicates continuous ports.

all: Indicates all ports.

【description】

port-isolation uplink ethernet the command is used to configure adding an uplink port.

no port-isolation uplink ethernet the command is used to delete the uplink port.

By default, all ports are uplink ports.

If two ports are not each other's uplink ports, they cannot communicate,and this creates isolation.

【example】

#Isolate port 0/0/2 from 0/0/3.

Switch(config)#interface ethernet 0/0/2

Switch(config-if-ethernet-0/0/2)#no port-isolation uplink ethernet 0/0/3

#Isolate port 0/0/3 from 0/0/2.

Switch(config)#interface ethernet 0/0/3

Switch(config-if-ethernet-0/0/3)#no port-isolation uplink ethernet 0/0/2

14.2 Port isolation monitoring and debugging the commands

14.2.1 show port-isolation

【the command】

show port-isolation [ethernet *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

port-id: Port number in the format of device number/slot number/port number, e.g. 0/0/1.

【description】

show port-isolation the command displays port isolation information.

【example】

#View the port isolation information of port 0/0/2.

Switch(config)#show port-isolation ethernet 0/0/2

Port-isolation information:

port : uplink list

e0/0/2 : e0/0/1-e0/1/4

show port-isolation ethernet 0/0/2 display field description.

Field	Description
Port	Port number
Uplink list	Uplink port number

14.2.2 debug port_isolation

【the command】

debug port_isolation

no debug port_isolation

【config-mode】

Global configuration mode

【parameter】

none

【description】

debug port_isolation the command enables the port isolation debugging function.

no debug port_isolation the command is used to disable the port isolation debugging function.

【example】

#Enables the port isolation debugging function.

Switch#configure terminal

Switch(config)#debug port_isolation

Chapter 15 VLAN

15.1 VLAN configuration the commands

15.1.1 vlan

【the command】

vlan *vlan-list*

no vlan *vlan-list*

【config-mode】

Global configuration mode

【parameter】

vlan-list: VLAN list, the value range is 1-4094, can be single or multiple VLAN IDs, the symbol "," indicates a non-contiguous VLAN ID, "-" indicates a continuous VLAN ID.

【description】

vlan *vlan-list* the command is used to create a VLAN and enter VLAN configuration mode.

no vlan the command is used to delete a VLAN.

By default, the system automatically creates VLAN 1.

Because VLAN 1 is the system default VLAN, it cannot be deleted.

Note:

When some functions depend on a VLAN, the VLAN cannot be deleted and an error message will be output.

【example】

#Create vlan 2.

Switch#configure terminal

Switch(config)#vlan 2

Switch(config-vlan-2)#exit

#Create vlan 2, 4- 5.

Switch#configure terminal

Switch(config)#vlan 2,4-5

Switch(config-vlan-range)#

15.1.2 switchport { all | ethernet port-id }

【the command】

switchport { all | ethernet *port-id* **[[to] ethernet** *port-id* **] }**

no switchport { all | ethernet *port-id* **[[to] ethernet** *port-id* **] }**

【config-mode】

VLAN configuration mode

【parameter】

All: Indicates all ports.

port-id: Port number in the format of device number/slot number/port number, e.g. 0/0/1.

to: Indicates continuous port.

【description】

switchport all the command is used to configure the current VLAN to contain all ports.

no switchport all the command is used to unconfigure the current VLAN to include all ports.

By default, VLAN1 contains all ports and the other VLANs do not contain all ports.

【example】

#Configure vlan 2 to include all ports.

Switch#configure terminal

Switch(config)#vlan 2

Switch(config-vlan-2)#switchport all

#Configure vlan 2 to include port 0/0/2, port 0/0/4-0/0/6.

Switch#configure terminal

Switch(config)#vlan 2

Switch(config-vlan-2)#switchport ethernet 0/0/2 ethernet 0/0/4 to ethernet 0/0/6

15.1.3 description

【the command】

description *value*

no description

【config-mode】

VLAN configuration mode

【parameter】

value: Name, supports up to 32 characters, no default configuration.

【description】

description the command is used to configure the name of the vlan.

no description the command is used to restore the default case to delete the configuration.

【example】

#Configure the name of vlan 2 as "administration".

Switch#configure terminal

Switch(config)#vlan 2

Switch(config-vlan-2)#description administration

15.1.4 switchport pvid

【the command】

switchport pvid *vlan-id*

no switchport pvid

【config-mode】

Port configuration mode

【parameter】

vlan-id: VLAN ID, the value range is 1-4094.

【description】

switchport pvid the command is used to configure the PVID of the port.

no switchport pvid the command is used to restore the default situation.

By default, the PVID of the port is 1.

The VLAN ID for the configured PVID must be created first.

【example】

#Configure the PVID of port 0/0/1 to be 1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#switchport pvid 1

15.1.5 switchport link-type

【the command】

switchport link-type { access | trunk | hybrid }

no switchport link-type

【config-mode】

Port configuration mode

【parameter】

access: Indicates that the link type is configured as access type.

trunk: Indicates that the configuration link type is hybrid type.

hybrid: Indicates that the link type is configured as hybrids type.

【description】

switchport link-type the command is used to configure the port link type.

no switchport link-type the command is used to restore the default situation.

By default, the link type of a port is hybrid type.

【example】

#Configure port 0/0/1 as Hybrid type.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#switchport link-type hybrid

15.1.6 switchport hybrid { untagged | tagged }vlan

【the command】

switchport hybrid { untagged | tagged } vlan { all | *vlan-list* }

no switchport hybrid vlan { all | *vlan-list* }

【config-mode】

Port configuration mode

【parameter】

untagged: Indicates that the port is joined to the specified VLAN in an untagged manner.

tagged: Indicates that the port is joined to the specified VLAN in an tagged manner.

all: Indicates all VLANs.

vlan-list: VLAN list, the value range is 1-4094, can be single or multiple VLAN IDs, the symbol "," indicates a non-contiguous VLAN ID, "-" indicates a continuous VLAN ID.

【description】

switchport hybrid { untagged | tagged } vlan the command is used to configure the hybrid port to join the VLAN.

no switchport hybrid vlan the command is used to configure the hybrid port to exit the VLAN.

By default, hybrid ports are joined to VLAN 1 as untagged.

This the command can only be configured if the port link type is Hybrid.

Note:

When configuring the hybrid port to join or exit the VLAN, make sure the link type of the port is Hybrid type, otherwise an error message will be output.

【example】

#hybrid port 0/0/1 is joined to vlan 2, 4-5 in untagged mode.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#switchport hybrid untagged vlan 2,4-5

15.1.7 switchport trunk allowed vlan

【the command】

switchport trunk allowed vlan { **all** | *vlan-list* }

no switchport trunk allowed vlan { **all** | *vlan-list* }

【config-mode】

Port configuration mode

【parameter】

all: Indicates all vlans.

vlan-list: vlan list, the value range is 1-4094, can be single or multiple VLAN IDs, the symbol "," indicates a non-contiguous VLAN ID, "-" indicates a continuous VLAN ID.

【description】

switchport trunk allowed vlan the command configures the Trunk port to allow the specified VLAN to pass.

no switchport trunk allowed vlan the command configures the trunk port to allow the specified VLAN to pass.

By default, Trunk ports allow vlan 1 to pass.

Note

When configuring a Trunk port to allow or disallow VLAN pass-through, ensure that the link type of the port is Trunk type, otherwise an error message will be output.

【example】

#Configure Trunk port 0/0/1 to allow VLAN 2, VLAN 4 - VLAN 5.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#switchport trunk allowed vlan 2,4-5

15.1.8 ingress filtering

【the command】

ingress filtering

no ingress filtering

【config-mode】

Port configuration mode

【parameter】

None

【description】

ingress filtering the command enables the ingress filtering function.

no ingress filtering the command is used to disable the ingress filtering function.

By default, ingress filtering is enabled on all ports.

【example】

#Configure port 0/0/1 to disable the ingress filtering function.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#no ingress filtering

15.1.9 ingress acceptable-frame

【the command】

ingress acceptable-frame { all | tagged | untagged }

no ingress acceptable-frame

【config-mode】

Port configuration mode

【parameter】

all: Indicates that all Tag messages and Untag messages are received.

tagged: Indicates that only tag messages are received and untag messages are discarded.

untagged: Indicates that only untag messages are received and tag messages are discarded.

【description】

ingress acceptable-frame the command configures the frames type to be received.

no ingress acceptable-frame the command is used to restore the default situation.

By default, the receive frame type is all, tag and untag messages are received.

【example】

#Configure port 0/0/1 to receive only Untag packets.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#ingress acceptable-frame untagged

15.2 VLAN monitoring and debugging the commands

15.2.1 show vlan

【the command】

show vlan [*vlan-id*]

【config-mode】

Arbitrary the command mode

【parameter】

vlan-id: vlan number, integer form, value range 1-4094.

【description】

show vlan the command displays the information of LAN.

【example】

#view the information of VLAN 2.

Switch(config)#show vlan 2

show VLAN information

VLAN name : @#$%546

VLAN ID : 2

VLAN status : static

VLAN member : e0/0/1-e0/1/4

Static tagged ports :

Static untagged Ports : e0/0/1-e0/1/4

Dynamic tagged ports :

show vlan display field description

field	description

VLAN name	VLAN name
VLAN ID	VLAN number
VLAN status	VLAN state: static, dynamic
VLAN member	Join members of this VLAN
Static tagged ports	Static tagged member ports
Static untagged Ports	Static untagged member ports
Dynamic tagged ports	dynamic tagged member ports

15.2.2 show vlan brief

【the command】

show vlan brief [*vlan-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

vlan-id: vlan number, integer form, value range 1-4094.

【description】

show vlan brief the command displays brief information about the vlan.

【example】

#View brief information about VLAN 1.

Switch(config)#show vlan brief 1

Vlan Name Status TagPort UntagPort

1 static e0/0/1-e0/1/4

show vlan brief display field description

field	description
VLAN	VLAN number
Name	VLAN name
Status	VLAN status
TagPort	Tagged member port
UntagPort	Untagged member port

15.2.3 show vlan brief interface

【the command】

show vlan brief interface [ethernet *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

port-id: Port number in the format of device number/slot number/port number, e.g. 0/0/1.

【description】

show vlan brief interface the command displays brief information about the vlan of the port.

【example】

#View VLAN summary information for all ports.

Switch(config)#show vlan brief interface

Port	Pri	LinkType	PVID	TagVlan	UntagVlan
e0/0/1	0	access	1		1
e0/0/2	0	access	1		1
e0/0/3	0	access	1		1
e0/0/4	0	access	1		1
e0/0/5	0	access	1		1
e0/0/6	0	access	1		1
e0/0/7	0	access	1		1
e0/0/8	0	access	1		1
e0/0/9	0	hybrid	1		1
e0/0/10	0	hybrid	1		1
e0/0/11	0	hybrid	1		1
e0/0/12	0	hybrid	1		1

……

Total entries: 28.

show vlan brief interface display field description

field	description
Port	port number
Pri	Port priority
LinkType	Port link type
PVID	Default VLAN

TagVlan	VLANs joined with the Tagged attribute
UntagVlan	VLANs joined with the Untagged attribute

15.2.4 show ingress interface

【the command】

show ingress interface [ethernet *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

port-id: Port number in the format of device number/slot number/port number, e.g. 0/0/1.

【description】

show ingress interface the command displays the configuration information of the ingress filtering function and the receive frame type function.

【example】

#View the ingress filtering function and receive frame type function configuration information of port 0/0/1.

Switch(config)#show ingress interface ethernet 0/0/1

Port Filtering Acceptable-frame

e0/0/1 enable all

show ingress interface ethernet 0/0/1 display field description.

field	description
Port	Port number

Filtering	Entry filter enable state：enable、disable
Acceptable-frame	Receive frame type：all、tagged、untagged

15.3 Mac-VLAN configuration the commands

15.3.1 mac-vlan mac-address

【the command】

mac-vlan mac-address *mac-address* **vlan** *vlan-id* **[priority** *value* **]**

no mac-vlan [mac-address *mac-address* **]**

【config-mode】

Global configuration mode

【parameter】

mac-address: MAC address, dotted hexadecimal form H:H:H:H:H:H.

vlan-id: VLAN ID, in the form of an integer, in the range 1-4094.

value: VLAN priority, integer form, in the range 0-7.

【description】

mac-vlan mac-address the command is used to configure MAC-VLAN table entries.

no mac-vlan mac-address the command is used to delete the specified MAC-VLAN table entry.

By default, no MAC VLAN table entry is configured.

【example】

#Configure MAC address 00:01:00:00:00:00:01 to be partitioned to VLAN 2.

Switch#configure terminal

Switch(config)#mac-vlan mac-address 00:01:00:00:00:01 vlan 2

15.4 Mac-VLAN monitoring and debugging the commands

15.4.1 show mac-vlan

【the command】

show mac-vlan [**mac-address** *mac-address*]

【config-mode】

Arbitrary the command mode

【parameter】

mac-address: MAC address, dotted hexadecimal form H:H:H:H:H:H.

【description】

show mac-vlan the command displays MAC-VLAN information.

【example】

#View MAC-VLAN information table entries.

Switch(config)#show mac-vlan

MAC Address VLAN ID Priority Status

00:01:00:00:00:01 2 0 active

Total active entries: 0.

Total inactive entries: 0.

show mac-vlan display field description.

field	description
MAC Address	MAC Address
VLAN ID	VLAN number

Priority	VLAN priority
Status	Status：active、inactive
Total active entries	Number of table entries in active state
Total inactive entries	Number of table entries in active state

15.5 IP-subnet-vlan configuration the commands

15.5.1 ip-subnet-vlan ipv4

【the command】

ip-subnet-vlan ipv4 *ip-address* **mask** *ip-mask* **vlan** *vlan-id* **[priority** *value* **]**

no ip-subnet-vlan [ipv4 *ip-address* **mask** *ip-mask* **]**

【config-mode】

Global configuration mode

【parameter】

ip-address: IP address, dotted decimal, e.g. 10.0.0.1.

ip-mask: Mask, in dotted decimal form, such as 255.0.0.0.

vlan-id: VLAN ID, in the form of an integer, in the range 1-4094.

value: VLAN priority, integer form, in the range 0-7.

【description】

ip-subnet-vlan ipv4 the command is used to configure IP subnet VLAN table entries.

no ip-subnet-vlan ipv4 the command deletes the specified IP subnet VLAN table entry.

By default, no IP subnet VLAN table entry is configured.

【example】

#Configure IP address 192.168.0.1 with mask 255.255.255.255 and divide it to VLAN 2.

Switch#configure terminal

Switch(config)#ip-subnet-vlan ipv4 192.168.0.1 mask 255.255.255.255 vlan 2

15.5.2 ip-subnet-vlan precede

【the command】

ip-subnet-vlan precede

no ip-subnet-vlan precede

【config-mode】

Global configuration mode

【parameter】

None

【description】

ip-subnet-vlan precede the command enables the IP subnet VLAN priority over the MAC-VLAN priority.

no ip-subnet-vlan ipv4 the command is used to restore the default configuration.

By default, the MAC-VLAN function takes precedence over the IP subnet VLAN function.

【example】

#Configure the enable IP subnet VLAN priority over MAC-VLAN function.

Switch#configure terminal

Switch(config)#ip-subnet-vlan precede

15.6 IP-subnet-vlan monitoring and debugging the commands

15.6.1 show ip-subnet-vlan

【the command】

show ip-subnet-vlan [ipv4 *ip-address* **mask** *ip-mask* **]**

【config-mode】

Arbitrary the command mode

【parameter】

ip-address: IP address, dotted decimal, e.g. 10.0.0.1.

mask-address: Mask, in dotted decimal form, such as 255.0.0.0.

【description】

show ip-subnet-vlan the command displays IP subnet VLAN information.

【example】

#View the IP subnet VLAN information table entries.

Switch(config)#show ip-subnet-vlan

The precedence of ip-subnet-based VLAN is higher than mac-based VLAN.

IP Address	IP Mask	VLAN ID	Priority	Status
192.168.0.1	255.255.255.255	2	0	active

Total active entries: 1.

Total inactive entries: 0.

show ip-subnet-vlan display field description.

field	description
IP Address	IP Address
IP Mask	IP Address Mask
VLAN ID	VLANs based on IP subnetting to

Priority	VLAN Priority
Status	Status：active、inactive
Total active entries	Number of table entries in active state
Total inactive entries	Number of table entries in inactive state

15.7 Protocol-VLAN configuration the commands

15.7.1 protocol-vlan profile frame-type ether-type

【the command】

protocol-vlan profile *profile-id* **frame-type** { **ethernet2 | llc | snap**} **ether-type** *type-value*

no protocol-vlan profile [*profile-id*]

【config-mode】

Global configuration mode

【parameter】

profile-id the number, in integer form, takes the value range 1-8.

ethernet2: Indicates an Ethernet II frame.

llc: Indicates an IEEE802.3 LLC (non-SNAP) frame.

snap: Indicates an IEEE802.3 SNAP frame.

type-value: Protocol number in hexadecimal format, value range 1 - FFFF.

【description】

protocol-vlan profile *profile-id* **frame-type** the command is used to configure the template.

no protocol-vlan profile [*profile-id*] the command is used to delete template.

By default, no protocol template is configured.

【example】

#Configure a protocol template number 1, encapsulation format llc, and protocol type 0x6000.

Switch#configure terminal

Switch(config)#protocol-vlan profile 1 frame-type llc ether-type 6000

15.7.2 protocol-vlan

【the command】

protocol-vlan

no protocol-vlan

【config-mode】

Port configuration mode

【parameter】

none

【description】

protocol-vlan the command is used to enable the protocol VLAN function.

no protocol-vlan the command is used to disable the protocol VLAN function.

By default, the port is not enabled for the protocol VLAN function.

The Protocol VLAN function takes effect only after the port enables the Protocol VLAN function and the protocol template to be matched is configured. The priority level of the protocol VLAN is higher than that of the port VLAN. As long as the port receives a protocol matching Untag message, the VLAN ID of the VLAN Tag added for it is the protocol VLAN corresponding to the matching template.

Note:

The port that enables the protocol VLAN function needs to join the corresponding protocol VLAN, otherwise the port cannot forward the messages of this VLAN, and the protocol-matching Untag messages will be discarded.

【example】

#Enables the protocol VLAN function of port 0/0/1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#protocol-vlan

15.7.3 protocol-vlan profile vlan

【the command】

protocol-vlan profile *profile-id* **vlan** *vlan-id* **[priority** *value* **]**

no protocol-vlan profile [*profile-id* **]**

【config-mode】

Port configuration mode

【parameter】

profile-id the number, in integer form, takes the value range 1-8.

vlan-id: VLAN ID value, in integer form, in the range of 1-4094.

value: VLAN priority, integer form, in the range 0-7.

【description】

protocol-vlan profile the command is used to apply protocol templates.

no protocol-vlan profile the command is used to cancel the application protocol template.

By default, the port does not have any protocol templates applied.

Multiple protocol templates can be applied on the same port.

The protocol vlan function takes effect only after the port applies the protocol template and enables the protocol vlan function of the port.

【example】

#Configure port 0/0/1 to apply protocol template 1 and divide it to VLAN 2.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#protocol-vlan profile 1 vlan 2

15.8 Protocol-VLAN monitoring and debugging the commands

15.8.1 show protocol-vlan profile

【the command】

show protocol-vlan profile [*profile-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

profile-id: Number, integer form, value range 1-8.

【description】

show protocol-vlan profile the command displays the protocol VLAN template configuration information.

【example】

#View the protocol VLAN template configuration information.

Switch(config)#show protocol-vlan profile

Profile Index Frame Type Ether Type Status

1 LLC 0x6000 active

Total active entries: 1.

Total inactive entries: 0.

show protocol-vlan profile display field description.

field	description

Profile Index	Protocol template number
Frame Type	Package format
Ether Type	Protocol Type
Status	Status：active、inactive
Total active entries	Number of table entries with active status
Total inactive entries	Number of table entries with inactive status

15.8.2 show protocol-vlan interface

【the command】

show protocol-vlan interface [ethernet *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

ethernet *port-id* : Display the configuration information of the protocol template matched by the specified port.

【description】

show protocol-vlan interface the command displays the configuration information of the protocol template matched by the port.

【example】

#View the configuration information of the protocol template matched on port 0/0/10.

Switch(config)#show protocol-vlan interface ethernet 0/0/10

Port AdminStatus Profile Index VLAN ID Priority ActionStatus

e0/0/10 enable 1 2 7 active

Total port entries: 1.

Total active action entries: 0.

Total inactive action entries: 0.

show protocol-vlan interface ethernet 0/0/10 display field description.

field	description
Port	Port number
AdminStatus	Enabled state
Profile Index	Protocol template number
VLAN ID	VLAN Number
Priority	VLAN Priority
ActionStatus	Status：active、inactive
Total port entries	Port Statistics
Total active action entries	Number of table entries with active status
Total inactive action entries	Number of table entries with inactive status

15.9 VLAN Swap configuration the commands

15.9.1 vlan swap

【the command】

vlan swap *start_vid end_vid swap-vid priority*

no vlan swap [*start_vid end_vid* **]**

【config-mode】

Port configuration mode

【parameter】

start_vid: Starting VLAN ID value, in integer form, in the range of 1-4094.

end_vid: End VLAN ID value, in integer form, in the range of 1-4094.

swap-vid the converted VLAN ID value, in integer form, takes a value in the range of 1-4094.

priority: VLAN priority, integer form, in the range 0-7.

【description】

vlan swap the command is used to configure vlan translation.

no vlan swap the command is used to remove vlan translation.

By default, the port is not configured for vlan translation.

The feature takes effect immediately after the vlan translation is configured, and there is no enable switch.

【example】

#Port 0/0/1 is configured with vlan translation: vlan 2-10 is converted to vlan 100.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#vlan swap 2 10 100 5

15.10 VLAN-Translate configuration the commands

15.10.1 vlan-translate-table { ingress | egress }

【the command】

vlan-translate-table{ ingress | egress } *start_vid end_vid translate_vid [priority* **]**

no vlan-translate-table{ ingress | egress } *start_vid end_vid*

【config-mode】

Port configuration mode

【parameter】

start_vid: Starting VLAN ID value, in integer form, in the range of 1-4094.

end_vid: End VLAN ID value, in integer form, in the range of 1-4094.

translate_vid the translated VLAN ID value, in integer form, takes a value in the range of 1-4094.

priority: VLAN priority, integer form, in the range 0-7.

ingress: Indicates translation at input.

egress: Indicates translation on output.

【description】

vlan-translate-table{ ingress | egress } the command is used to configure the VLAN translation table.

no vlan-translate-table{ ingress | egress } the command is used to delete the VLAN translation table.

By default, no translation table is configured.

【example】

#Port 0/0/1 is configured with an ingress translation table: vlan 2-10 is translated to vlan 100.

Switch#configure terminal

Switch(config)interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#vlan-translate-table ingress 2 10 100

15.10.2 vlan-translate { ingress | egress }

【the command】

vlan-translate { ingress | egress }

no vlan-translate { ingress | egress }

【config-mode】

Port configuration mode

【parameter】

none

【description】

vlan-translate ingress the command is used to enable the VLAN translation function.

no vlan-translate ingress the command is used to disable the VLAN translation function.

By default, the port is not enabled for VLAN translation.

【example】

#Enables the VLAN translation function of port 0/0/1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#vlan-translate-table

15.11 VLAN-Translate monitoring and debugging the commands

15.11.1 show vlan-translate-table

【the command】

show vlan-translate-table { ingress | egress }

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show vlan-translate-table { ingress | egress } the command displays the VLAN translation table configuration information.

【example】

#View the VLAN translation table configuration information for ingress.

Switch(config)#show vlan-translate-table ingress

Port StartVid EndVid NewVid NewPriority Status

Total active entries: 0.

Total inactive entries: 0.

show vlan-translate-table ingress display field description

field	description
Port	Port number
StartVid	Starting VLAN ID
EndVid	End VLAN ID
NewVid	Translated VLNA ID
NewPriority	Translated priority
Status	Status：active、inactive
Total active entries	Number of table entries in active state
Total inactive entries	Number of table entries in inactive state

15.11.2 show vlan-translate

【the command】

show vlan-translate [ethernet *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

ethernet *port-id*: Displays the protocol template configuration information matched by the specified port.

【description】

show protocol-vlan interface the command displays the configuration information of the protocol template matched by the port.

【example】

#View the configuration information of the protocol template matched on port 0/0/10.

Switch(config)#show vlan-translate ethernet 0/0/1

Port Ingress Egress

e0/0/1 disable disable

Total port entries: 1.

show vlan-translate ethernet display field description

field	description
Port	Port number
Ingress	Ingress direction enable state
Egress	Egress direction enable state
Total port entries	Statistical table items

Chapter 16 QinQ

16.1 QinQ configuration the commands

16.1.1 qinq

【the command】

qinq

no qinq

【config-mode】

Global configuration mode

【parameter】

none

【description】

qinq the command is used to enable QinQ function.

no qinq the command is used to disable the QinQ function.

By default, the QinQ function is disabled.

【example】

#Global enablement of QinQ function

Switch#configure terminal

Switch(config)#qinq

16.1.2 qinq mode

【the command】

qinq mode { customer | uplink }

no qinq mode

【config-mode】

Interface configuration mode

【parameter】

customer: Indicates the customer mode, connecting to the user side.

uplink: Indicates uplink mode, connecting ISP side.

【description】

qinq mode the command is used to configure the QinQ mode.

no qinq mode the command is used to restore the default configuration.

By default, all ports are in uplink mode

【example】

#Configure the QinQ mode of port 0/0/2 to customer mode.

Switch(config)#interface ethernet 0/0/2

Switch(config-if-ethernet-0/0/2)#qinq mode customer

16.1.3 vlan insert

【the command】

vlan insert *start-vid end-vid service-vid priority*

no vlan insert { all | *start-vid end-vid* **}**

【config-mode】

Interface configuration mode

【parameter】

start-vid: Configure the CVLAN starting VLAN ID in integer form, in the range 1-4094.

end-vid: Configure the CVLAN end VLAN ID in integer form with a value range of 1-4094.

service-vid: SVLAN ID, integer form, value range 1-4094.

priority: Priority, integer form, takes values in the range 1-7.

all: Indicates all table entries.

【description】

vlan insert the command is used to configure flexible QinQ forwarding rules.

no vlan insert the command is used to delete the flexible QinQ forwarding rules.

By default, the port is not configured with flexible QinQ forwarding rules

When a received message does not match the flexible QinQ forwarding rule, it is forwarded using static QinQ with the outer Tag plus the ingress PVID.

【example】

#Configure port 0/0/2 incoming messages to match CVLAN 1-10 to be forwarded using SVLAN 11 priority 7.

Switch(config)#interface ethernet 0/0/2

Switch(config-if-ethernet-0/0/2)#vlan insert 1 10 11 7

16.1.4 vlan pass-through

【the command】

vlan pass-through *start-vid end-vid*

no vlan pass-through { all | *start-vid end-vid* **}**

【config-mode】

Interface configuration mode

【parameter】

start-vid: Configure the CVLAN starting VLAN ID in integer form, in the range 1-4094.

end-vid: Configure the CVLAN end VLAN ID in integer form with a value range of 1-4094.

all: Indicates all table entries.

【description】

pass-through the command is used to configure the pass-through VLAN rule.

no pass-through the command is used to delete the pass-through VLAN rule.

By default, the port is not configured with a pass-through VLAN rule.

If the port is not working in customer mode, the configuration will fail.

【example】

#Configure port 0/0/2 to not use QinQ forwarding for messages with CVLAN between 20 and 30.

Switch(config)#interface ethernet 0/0/2

Switch(config-if-ethernet-0/0/2)#vlan pass-through 20 30

16.1.5 qinq inner-tpid

【the command】

qinq inner-tpid *tpid-value*

no qinq inner-tpid

【config-mode】

Global configuration mode

【parameter】

tpid-value: TPID value, hexadecimal number, range 1 - FFFF.

【description】

qinq inner-tpid the command is used to configure the TPID of the inner VLAN Tag.

no qinq inner-tpid the command is used to restore the default configuration.

By default, the TPID value of the inner VLAN Tag is 0x8100, indicating 802.1Q protocol packets.

【example】

#Configure the TPID value of the Inner Layer VLAN Tag to 0x9100.

Switch#configure terminal

Switch(config)#qinq inner-tpid 9100

16.1.6 qinq outer-tpid

【the command】

qinq outer-tpid *tpid-value*

no qinq outer-tpid

【config-mode】

Global configuration mode

【parameter】

tpid-value: TPID value, hexadecimal number, in the range of 1 to FFFF.

【description】

qinq inner-tpid the command is used to configure the TPID of the outer VLAN Tag.

no qinq inner-tpid the command is used to restore the default configuration.

By default, the TPID value of the outer VLAN Tag is 0x8100, indicating 802.1Q protocol packets.

【example】

#Configure the TPID value of the outer VLAN Tag to 0x9100.

Switch#configure terminal

Switch(config)#qinq outer-tpid 9100

16.2 QinQ monitoring and debugging the commands

16.2.1 show qinq

【the command】

show qinq

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show qinq the command to view QinQ configuration information.

【example】

#View QinQ configuration information.

Switch(config)#show qinq

Global Enabled: enable

Inner tpid: 0x9100

Outer tpid: 0x8100

Port : Mode

e0/0/1 : customer

e0/0/2 : customer

e0/0/3 : uplink

……

show qinq display field description

field	description
Global Enabled	Enable state
Inner tpid	Inner Label TPID
Outer tpid	Outer Label TPID
Port	Port
Mode	operating mode

Chapter 17 MAC address management

17.1 MAC address management configuration the commands

17.1.1 mac-address-table age-time

【the command】

mac-address-table age-time { *aging-time-value* | **disable** }

no mac-address-table age-time

【config-mode】

Global configuration mode

【parameter】

aging-time-value: Aging time, in integer form, in the range 10-1000000, in seconds.

disable: Indicates that the aging function is disabled.

【description】

mac-address-table age-time the command to configure the aging time of the MAC address.

By default, the aging time for MAC addresses is 1200 second.

【example】

#Configure the MAC address aging time to 600 seconds.

Switch#configure terminal

Switch(config)#mac-address-table aging-time 600

17.1.2 mac-address-table max-mac-count

【the command】

mac-address-table max-mac-count *count-value*

no mac-address-table max-mac-count

【config-mode】

Port configuration mode

【parameter】

count-value: MAC limit, in integer form, ranging from 1 to 16384.

【description】

mac-address-table max-mac-count the command configures the dynamic MAC address learning upper limit.

no mac-address-table max-mac-count the command to restore the default configuration.

By default, the port is configured with a dynamic MAC address learning upper limit of 16384.

【example】

#Configure the limit of MAC addresses to be learned 200 on port 0/0/1 to.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mac-address-table max-mac-count 200

17.1.3 mac-address-table permanent

【the command】

mac-address-table permanent *mac-address* **interface ethernet** *port-id* **vlan** *vlan-id*

no mac-address-table permanent *mac-address* **[interface ethernet** *port-id* **] vlan** *vlan-id*

no mac-address-table permanent { interface ethernet *port-id* **| vlan** *vlan-id* **}**

【config-mode】

Global configuration mode

【parameter】

mac-address: MAC address in dotted hexadecimal form.

vlan-id: VLAN ID, integer form, value range 1-4094.

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

mac-address-table permanent the command to create a permanent MAC address table entry.

no mac-address-table permanent the command deletes the permanent MAC address table entry.

Permanent MAC address table entries that do not age and remain after a save reboot.

【example】

#Create a permanent MAC address table entry with a MAC of 00:0e:5e:12:34:56, a VLAN of VLAN 3, and an outgoing port 0/0/1

Switch#configure terminal

Switch(config)#mac-address-table permanent 00:0e:5e:12:34:56 interface ethernet 0/0/1 vlan 3

17.1.4 mac-address-table blackhole

【the command】

mac-address-table blackhole *mac-address* **vlan** *vlan-id*

no mac-address-table blackhole [*mac-address* **] vlan** *vlan-id*

【config-mode】

Global configuration mode

【parameter】

mac-address: MAC address in dotted hexadecimal form.

vlan-id: VLAN ID, integer form, value range 1-4094.

【description】

mac-address-table blackhole the command to create a blackhole MAC address table entry.

no mac-address-table blackhole: Used to delete the Blackhole MAC address table entry.

【example】

#Create a Blackhole MAC address table entry:mac 00:0e:5e:12:34:56 VLAN 3.

Switch#configure terminal

Switch(config)#mac-address-table blackhole 00:0e:5e:12:34:56 vlan 3

17.1.5 mac-address-table static

【the command】

mac-address-table static *mac-address* **interface ethernet** *port-id* **vlan** *vlan-id*

no mac-address-table static *mac-address* **[interface ethernet** *port-id* **] vlan** *vlan-id*

no mac-address-table static { interface ethernet *port-id* **| vlan** *vlan-id* **}**

【config-mode】

Global configuration mode

【parameter】

mac-address: MAC address in dotted hexadecimal form.

vlan-id: VLAN ID, integer form, value range 1-4094.

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

mac-address-table static the command to create a static MAC address table entry.

no mac-address-table static the command deletes a static MAC address table entry.

Static MAC address table entries do not age, configurations cannot be saved, and configurations disappear after reboot.

【example】

#Create a static MAC address table entry with a MAC address of 00:0e:5e:12:34:56, a VLAN of VLAN 3, and an outgoing port 0/0/1.

Switch#configure terminal

Switch(config)#mac-address-table static 00:0e:5e:12:34:56 interface ethernet 0/0/1 vlan 3

17.1.6 mac-address-table dynamic

【the command】

mac-address-table dynamic *mac-address* **interface ethernet** *port-id* **vlan** *vlan-id*

no mac-address-table dynamic *mac-address* **[interface ethernet** *port-id* **] vlan** *vlan-id*

no mac-address-table dynamic { interface ethernet *port-id* **| vlan** *vlan-id* **}**

【config-mode】

Global configuration mode

【parameter】

mac-address: MAC address in dotted hexadecimal form.

vlan-id: VLAN ID, integer form, value range 1-4094.

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

mac-address-table dynamic the command to create a dynamic MAC address table entry.

no mac-address-table dynamic the command deletes a dynamic MAC address table entry.

【example】

#Create a dynamic MAC address table entry with a MAC address of 00:0e:5e:12:34:56, a VLAN of VLAN 3, and an outgoing port 0/0/1.

Switch#configure terminal

Switch(config)#mac-address-table dynamic 00:0e:5e:12:34:56 interface ethernet 0/0/1 vlan 3

17.1.7 mac-address-table learning

【the command】

mac-address-table learning

no mac-address-table learning

【config-mode】

Global configuration mode/Port configuration mode/VLAN configuration mode

【parameter】

none

【description】

mac-address-table learning the command enables the MAC address learning function.

no mac-address-table learning the command disables the MAC address learning function.

By default, the MAC address learning function is enabled.

【example】

#Enable the MAC address learning function on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mac-address-table learning

#Disable the MAC address learning function for VLAN 2.

Switch(config)#vlan 2

Switch(config-vlan-2)#no mac-address-table learning

17.1.8 no mac-address-table

【the command】

no mac-address-table [interface ethernet *port-id* **| vlan** *vlan-id* **|** *mac-address* **[interface ethernet** *port-id* **] vlan** *vlan-id* **]**

【config-mode】

Global configuration mode

【parameter】

port-id: Port number, the value range is determined by the device model, for example: 0/0/1.

vlan-id: VLAN ID, integer form, value range 1-4094.

mac-address: MAC address in dotted hexadecimal form.

【description】

no mac-address-table the command clears the static and dynamic MAC table entries .

This the command does not clear permanent and blackhole MAC addresses.

【example】

#Binding clears all dynamic and static MAC address table entries.

Switch#configure terminal

Switch(config)#no mac-address-table

Do you want to delete all dynamic and static mac addresses(y/n)? [n]y

17.1.9 no mac-address-table express

【the command】

no mac-address-table [interface ethernet *port-id* **] express**

【config-mode】

Global configuration mode

【parameter】

port-id: Port number, the value range is determined by the device model, for example: 0/0/1.

【description】

no mac-address-table express the command to clear the cache MAC address table.

【example】

#Clear Cache.

Switch#configure terminal

Switch(config)#no mac-address-table express

17.1.10 unknown-discard src-mac

【the command】

unknown-discard src-mac

no unknown-discard src-mac

【config-mode】

Port configuration mode

【parameter】

none

【description】

unknown-discard src-mac the command enables the function of discarding messages whose source MAC is unknown.

no unknown-discard src-mac the command disables the function of discarding messages whose source MAC is unknown.

By default, the function of dropping messages with unknown source MAC is disabled, that is, forwarding messages with unknown source MAC.

【example】

#Enable port 0/0/1 to drop packets of unknown origin

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#unknown-discard src-mac

17.1.11 local-switch

【the command】

local-switch

no local-switch

【config-mode】

Port configuration mode

【parameter】

none

【description】

local-switch the command enables local switch function.

no local-switch the command disables local switch function.

By default, the function is disabled. Flooded unknown messages to any port without ingress port.

【example】

#Enable port 0/0/1 unknown message forwarding from ingress function.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#local-switch

17.2 MAC address management monitoring and debugging the commands

17.2.1 show mac-address aging-time

【the command】

show mac-address aging-time

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show mac-address aging-time the command to view the dynamic MAC address aging time.

【example】

#View the dynamic MAC address aging time.

Switch(config)#show mac-address-table age-time

mac address table agingtime is 1200 seconds.

17.2.2 show mac-address-table

【the command】

show mac-address-table [permanent | static | dynamic] [{ ethernet | eth-trunk } *port-id* **] [vlan** *vlan-id* **]**

show mac-address-table blackhole [vlan *vlan-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

blackhole: Indicates a blackhole MAC address table entry.

permanent: Indicates a permanent MAC address table entry.

static: Indicates a static MAC address table entry.

dynamic: Indicates a dynamic MAC address table entry.

vlan-id: VLAN ID, integer form, value range 1-4094.

eth-trunk: Indicates the link aggregation port.

port-id: Port number, Ethernet port format such as 0/0/1, aggregation group port number configuration range 1-16.

【description】

show mac-address-table the command to view the MAC address table entry information.

【example】

#View MAC address table entry information.

Switch(config)#show mac-address-table

MAC Address VLAN ID port status

00:00:00:00:00:01 1 0/0/1 static

show mac-address-table display field description

field	description
MAC Address	MAC address
VLAN ID	VLAN number
Port	Port number
Status	Types：static、dynamic、permanent、blackhole

17.2.3 show mac-address-table mac-address

【the command】

show mac-address-table *mac-address* **[vlan** *vlan-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

mac-address: MAC address in dotted hexadecimal form.

vlan-id: VLAN ID, integer form, value range 1-4094.

【description】

show mac-address-table *mac-address*：the command to view the MAC address table entry information for the specified MAC address.

【example】

#View information about MAC address table entries with MAC address 00:00:00:00:00:01.

Switch(config)#show mac-address-table 00:00:00:00:00:01

MAC Address VLAN ID port status

00:00:00:00:00:01 1 0/0/1 static

show mac-address-table display field description

field	description
MAC Address	MAC address
VLAN ID	VLAN number
Port	Port number

Status	Types：static、dynamic、permanent、blackhole

17.2.4 show mac-address-table vlan

【the command】

show mac-address-table vlan *vlan-id*

【config-mode】

Arbitrary the command mode

【parameter】

vlan-id: VLAN ID, integer form, value range 1-4094.

【description】

show mac-address-table vlan： the command to view the MAC address table entry information for the specified VLAN.

【example】

#View the MAC address table entry information for VLAN 1.

Switch(config)#show mac-address-table vlan 1

MAC Address VLAN ID port status

00:00:00:00:00:01 1 0/0/1 static

show mac-address-table vlan 1display field description

field	description
MAC Address	MAC address
VLAN ID	VLAN number
Port	Port number

Status	Types：static、dynamic、permanent、blackhole

17.2.5 show mac-address-table learning

【the command】

show mac-address-table learning { interface [ethernet *port-id* **] | vlan [** *vlan-id* **] }**

【config-mode】

Arbitrary the command mode

【parameter】

vlan-id: VLAN ID, integer form, value range 1-4094.

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

show mac-address-table learning the command to view the MAC address learning enable configuration.

【example】

#View the MAC address learning enable configuration for port 0/0/1.

Switch(config)#show mac-address-table learning interface ethernet 0/0/1

Port status

0/0/1 enable

show mac-address-table learning display field description

field	description
Port	Port number
Status	Enable state

17.2.6 show mac-address-table max-mac-count interface

【the command】

show mac-address-table max-mac-count interface [ethernet *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

show mac-address-table max-mac-count interface :the command is used to view the dynamic MAC address learning upper limit value.

【example】

#View the dynamic MAC address learning upper limit for port 0/0/1.

Switch(config)#show mac-address-table max-mac-count interface ethernet 0/0/1

Port Mac address max count

e0/0/1 16384

show mac-address-table max-mac-count display field description

field	description
Port	Port number
Mac address max count	MAC Limit Number

17.2.7 show unknown-discard src-mac

【the command】

show unknown-discard src-mac

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show unknown-discard src-mac the command is used to view the configuration information of the discard source MAC unknown message function.

【example】

#View the configuration information of the discard source MAC unknown message feature.

Switch(config)#show unknown-discard src-mac

Port	Srcmac unknown discard status
0/0/1	enable
0/0/2	disable
0/0/3	disable
0/0/4	disable
0/0/5	disable
0/0/6	disable

……

show unknown-discard src-mac display field description

field	description
Port	Port number
Srcmac unknown discard status	Enable state: disable、enable

17.2.8 show local-switch

【the command】

show local-switch

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show local-switch the command to view configuration information.

【example】

#View local-switch configuration information.

Switch(config-if-ethernet-0/0/1)#show local-switch

port local-switch-state

e0/0/1 disable

e0/0/2 disable

e0/0/3 disable

e0/0/4 disable

e0/0/5 disable

e0/0/6 disable

e0/0/7 disable

e0/0/8 disable

……

Total entries: 54.

show local-switch display field description

field	description
Port	Port number
local-switch-state	Enable state: disable、enable

Chapter 18 Spanning tree protocol

18.1 STP/RSTP configuration the commands

18.1.1 stp

【the command】

stp

no stp

【config-mode】

Global configuration mode

【parameter】

none

【description】

stp the command enables the STP function.

no stp the command disables the STP function.

By default, the global STP function is disabled and the port STP function is enabled.

【example】

#Enable the global STP function.

Switch#configure terminal

Switch(config)#stp

#Enable the STP function on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp

18.1.2 stp mode

【the command】

stp mode { stp | mstp | rstp }

【config-mode】

Global configuration mode

【parameter】

stp: Configure the spanning tree operating mode as STP mode.

mstp: Configure the spanning tree operating mode as MSTP mode.

rstp: Configure the spanning tree operating mode as RSTP mode.

【description】

stp mode the command configures the spanning tree operating mode.

no stp mode the command to restore the default situation.

By default, the spanning tree operating mode is RSTP mode.

In STP mode, each port of the device will send STP BPDU messages outward, in RSTP mode, each port of the device will send RSTP BPDU messages outward, and in MSTP mode, each port of the device will send MSTP BPDU messages outward. MSTP is backward compatible with STP and RSTP, and RSTP is backward compatible with STP, i.e., a port working in MSTP mode will automatically migrate to work in the corresponding compatibility mode when it is found to be connected to a device running STP or RSTP, and a port working in RSTP mode will automatically migrate to work in the STP compatibility mode when it is found to be connected to a device running STP.

Note:

When Spanning Tree is globally enabled, modifications to the Spanning Tree operating mode will cause a restart of the protocol, which may result in a brief interruption of the network.

【example】

#Configure the spanning tree operating mode as STP mode.

Switch#configure terminal

Switch(config)#stp mode stp

18.1.3 stp priority

【the command】

stp priority *priority-value*

no stp priority

【config-mode】

Global configuration mode

【parameter】

priority-value: Priority, in integer form, with values in the range 0-61440, is issued successfully as a multiple of 4096.

【description】

stp priority the command to configure the system priority of the device.

no stp priority the command to restore the default configuration.

By default, the system priority is 32768.

【example】

#Configure the system priority to 8192.

Switch#configure terminal

Switch(config)#stp priority 8192

18.1.4 stp port-priority

【the command】

stp port-priority *priority-value*

no stp port-priority

【config-mode】

Port configuration mode

【parameter】

priority-value: Configuration priority. in integer form. in the range 0-240. the downstream success is a multiple of 16.

【description】

stp port-priority the command to configure port priority.

no stp port-priority the command to restore the default configuration.

By default, the port priority is 128.

【example】

#Configure port 0/0/1 priority as 64.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp port-priority 64

18.1.5 stp forward-time

【the command】

stp forward-time *time-value*

no stp forward-time

【config-mode】

Global configuration mode

【parameter】

time-value the forwarding delay time value, in integer form, ranging from 4 to 30 in seconds.

【description】

stp forward-time the command to configure the forwarding delay time for STP.

no stp forward-time the command to restore the default situation.

By default, the forwarding delay for STP is 15 seconds.

When the network topology changes, the spanning tree needs to be recalculated, and it takes some time for the new configuration messages to spread throughout the network. If the newly elected root port and the designated port forward the data immediately, it may cause a temporary path loopback. Therefore, before the ports forward the data again, they have to go through an intermediate state (learning), and the intermediate state can enter the forwarding state only after the forwarding delay time. Use this the command to configure the forwarding delay time to ensure that the new

configuration message has been transmitted throughout the network. When the network topology changes infrequently, the delay time can be reduced appropriately, and vice versa.

Note:

max-age,hello-time and forward-time must satisfy the following relationship:

2 * (HelloTime + 1) <= MaxAge <= 2 * (ForwardDelay - 1)

【example】

#Configure the forward-time value for STP to be 20 seconds.

Switch#configure terminal

Switch(config)#stp forward-time 20

18.1.6 stp hello-time

【the command】

stp hello-time *time-value*

no stp hello-time

【config-mode】

Global configuration mode

【parameter】

time-value the time interval for sending BPDUs, in integer form, ranging from 1 to 10, in seconds.

【description】

stp hello-time the command is used to configure the Hello Time of STP, i.e., the time interval for sending BPDUs.

no stp hello-time the command to restore the default situation.

By default, the Hello Time for STP is 2 seconds.

Hello Time refers to the time interval for the root bridge to send BPDU messages to other bridges at regular intervals. Appropriate Hello Time configuration can ensure that the device can detect link failures in the network in time without occupying too much network resources. If the configured Hello Time is too long, when the link loses packets, the device

will mistakenly think that the link is faulty, thus triggering the recalculation of the spanning tree. If the configured Hello Time is too short, the device will frequently send repeated configuration messages, which increases the processing burden of the device and wastes the network resources.

Note:

l max-age, hello-time and forward-time must satisfy the following relationship:

2 * (HelloTime + 1) <= MaxAge <= 2 * (ForwardDelay - 1)

【example】

#Configure the Hello Time value for STP to be 3 seconds.

Switch#configure terminal

Switch(config)#stp hello-time 3

18.1.7 stp max-age

【the command】

stp max-age *time-value*

no stp max-age

【config-mode】

Global configuration mode

【parameter】

time-value: Max Age time, ranging from 6 to 40 in seconds.

【description】

stp max-age the command configures the maximum retention time of BPDU configuration messages on the device.

no stp max-age the command to restore the default situation.

By default, the STP max-age is 20 seconds.

The Max Age time is used to determine whether the received BPDU configuration message is timeout or not, and the timeout configuration message will be discarded and cannot be used for spanning tree calculation. If the Max Age time is

too long, the device may not be able to detect link failure in time and recalculate the spanning tree in time, which reduces the adaptive capability of the network. If the Max Age time is too short, the device will calculate the spanning tree frequently, and it may mistake the network congestion for link failure.

Note:

l max-age, hello-time and forward-time must satisfy the following relationship:

2 * (HelloTime + 1) <= MaxAge <= 2 * (ForwardDelay - 1)

【example】

#Configure the STP max-age value to 30 seconds.

Switch#configure terminal

Switch(config)#stp max-age 30

18.1.8 stp portfast

【the command】

stp portfast { autoedge | edgeport | disable }

no stp portfast

【config-mode】

Port configuration mode

【parameter】

autoedge: Indicates that it automatically detects whether it is an edge port.

edgeport: Indicates that it is forced to be an edge port.

disable: Indicates that it is forced to be a non-edge port.

【description】

stp portfast the command to configure whether the port is an edge port.

no stp portfast the command to restore the default situation.

By default, all ports are autoedge.

【example】

#Configure port 0/0/1 as an edge port.

Switch(config-aaa)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp portfast edgeport

18.1.9 stp link-type

【the command】

stp link-type { auto | point-to-point | shared }

no stp link-type

【config-mode】

Port configuration mode

【parameter】

auto: Indicates that the link connected to this port is automatically detected as a point-to-point link.

point-to-point: Indicates that the link to the current port is a point-to-point link.

shared: Indicates that the link connected to the current port is a shared link.

【description】

stp link-type the command to configure the link type of the port.

no stp link-type the command to restore the default situation.

By default, the link type is configured as auto.

Note:

l The link type of the port should be configured according to the actual physical link. if the actual physical link of the port is not a point-to-point link and is incorrectly configured as a point-to-point link, a temporary loop may be introduced.

2 When the link type of the local port is a shared link type, the local port does not support the edge port auto-recognition function, and if the peer port carries out the edge port auto-recognition, it may cause the peer port to

be incorrectly recognized as an edge port.

【example】

#Configure the link type of port 0/0/5 as a point-to-point link.

Switch(config-aaa)#interface ethernet 0/0/5

Switch(config-if-ethernet-0/0/1)#stp link-type point-to-point

18.1.10 stp bpdu-filter

【the command】

stp bpdu-filter

no stp bpdu-filter

【config-mode】

Global configuration mode/Port configuration mode

【parameter】

none

【description】

stp bpdu-filter the command enables the BPDU filtering function.

no stp bpdu-filter the command to disable the BPDU filtering function.

By default, BPDU filtering is disabled.

The BPDU Filter function of a port takes effect only on the edge port. The edge port receives BPDU messages from other ports and becomes a non-edge port again. After the BPDU Filter function of a port is enabled, the port will not send or receive BPDU message.

Note:

Whether the spanning tree port BPDU Filter function takes effect or not is prioritized by the port configuration. In port none configuration, if the global BPDU Filter is on, the port BPDU Filter function is on by default, and vice versa, the port BPDU Filter function is off by default.

【example】

#Configure to enable BPDU filtering on port 0/0/1.

Switch(config-aaa)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp bpdu-filter

18.1.11 stp bpdu-guard

【the command】

stp bpdu-guard

no stp bpdu-guard

【config-mode】

Port configuration mode

【parameter】

none

【description】

stp bpdu-guard the command enables the port BPDU protection function.

no stp bpdu-guard the command disables the port BPDU protection function.

By default, port BPDU protection is disabled.

The BPDU Guard function of a port takes effect only on the edge port. The edge port receives BPDU messages from other ports and becomes a non-edge port again.

After the BPDU Guard function is enabled, if the edge port receives BPDU messages, it will be shut down, and at the same time, the user will be prompted with a log message to restart the port to recover. For the identified edge port, it is recommended to enable the BPDU Guard function on the port to avoid malicious attacks by forging BPDU messages.

Note:

Whether the spanning tree port BPDU Guard function takes effect or not is prioritized by the port configuration. In port none configuration, if global BPDU Guard is on, the port BPDU Guard function is on by default, and vice versa.

【example】

#Configure to enable BPDU protection on port 0/0/1.

Switch(config-aaa)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp bpdu-guard

18.1.12 stp transit-limit

【the command】

stp transit-limit *max-num-value*

no stp transit-limit

【config-mode】

Port configuration mode

【parameter】

max-num-value: Maximum number of messages, in integer form, in the range 1-255.

【description】

stp transit-limit the command is used to configure the maximum number of messages allowed to send BPDUs during Hello Time.

no stp transit-limit the command to restore the default situation.

By default, up to 3 BPDU messages are sent during Hello Time.

【example】

#Configure port 0/0/1 to send a maximum of 10 BPDU messages during Hello Time.

Switch(config-aaa)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp transmit-limit 10

18.1.13 stp loop-guard

【the command】

stp loop-guard

no stp loop-guard

【config-mode】

Port configuration mode

【parameter】

none

【description】

stp loop-guard the command is used to configure the enable port ring protection function.

no stp loop-guard the command to restore the default situation.

By default, the port ring protection function is disabled.

【example】

#Enable ring protection on port 0/0/1.

Switch(config-aaa)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp loop-guard

18.1.14 stp root-guard

【the command】

stp root-guard

no stp root-guard

【config-mode】

Port configuration mode

【parameter】

none

【description】

stp root-guard the command is used to configure the enable root port protection function.

no stp root-guard the command to restore the default situation.

By default, root port protection is disabled.

【example】

#Enable root port protection for port 0/0/1.

Switch(config-aaa)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp root-guard

18.1.15 stp root-guard action

【the command】

stp root-guard action { block-port | drop-bpdu }

【config-mode】

Global configuration mode

【parameter】

block-port: Indicates a blocked port.

drop-bpdu: Indicates that the BPDU message is discarded.

【description】

stp root-guard action the command to configure the processing behavior of Root Guard.

By default, the processing is block-port.

【example】

#Configure the processing behavior of Root Guard as drop-bpdu.

Switch#configure terminal

Switch(config)#stp root-guard action drop-bpdu

18.1.16 stp pathcost-standard

【the command】

stp pathcost-standard { dot1d-1998 | dot1t }

no stp pathcost-standard

【config-mode】

Global configuration mode

【parameter】

dot1d-1998: Indicates that the default path overhead is calculated according to the IEEE 802.1D-1998 standard.

dot1t: Indicates that the default path overhead is calculated according to the IEEE 802.1t standard.

【description】

stp pathcost-standard the command to configure the criteria for calculating the default path overhead.

no stp pathcost-standard the command to restore the default situation.

By default, the dotlt standard is used.

【example】

#Configure the default path spend calculation method to use the dot1d-1998 standard.

Switch#configure terminal

Switch(config)#stp pathcost-standard dot1d-1998

18.1.17 stp tc-protection

【the command】

stp tc-protection

no stp tc-protection

【config-mode】

Global configuration mode

【parameter】

none

【description】

stp tc-protection the command enables the TC BPDU attack protection function

no stp tc-protection the command to restore the default situation.

By default, enable TC BPDU attack protection is disabled.

【example】

#Configure the enable TC BPDU attack protection function.

Switch#configure terminal

Switch(config)#stp tc-protection

18.1.18 stp tc-protection interval

【the command】

stp tc-protection interval *interval-value*

no stp tc-protection interval

【config-mode】

Global configuration mode

【parameter】

interval-value: Takes a value, in integer form, in the range 1-255, in seconds.

【description】

stp tc-protection interval the command configures the time period for processing TC BPDU messages.

no stp tc-protection interval the command to restore the default situation.

By default, the time period for processing TC BPDU messages is 10 seconds.

【example】

#Configure the processing time period for TC BPDU messages to be 20 seconds.

Switch#configure terminal

Switch(config)#stp tc-protection interval 20

18.1.19 stp tc-protection threshold

【the command】

stp tc-protection threshold *value*

no stp tc-protection threshold

【config-mode】

Global configuration mode

【parameter】

value: Takes a value, in integer form, in the configuration range 1-255.

【description】

stp tc-protection threshold the command is used to configure the number of times a TC message is processed in a time period.

no stp tc-protection threshold the command to restore the default situation.

By default, the maximum number of processes in a cycle is 6.

【example】

#Configure the maximum number of times to process TC BPDU messages to 5.

Switch#configure terminal

Switch(config)#stp tc-protection threshold 5

18.1.20 stp time-factor

【the command】

stp time-factor *time-factor-value*

no stp time-factor

【config-mode】

Global configuration mode

【parameter】

time-factor-value: Takes a value, in integer form, in the configuration range 1-10.

【description】

stp time-factor the command to configure the timeout factor.

no stp time-factor the command to restore the default situation.

By default, the default timeout factor is equal to 3.

【example】

#Configure the timeout factor to be equal to 6.

Switch#configure terminal

Switch(config)#stp time-factor 6

18.1.21 stp cost

【the command】

stp cost *cost-value*

no stp cost

【config-mode】

Port configuration mode

【parameter】

cost-value: Takes a value, in integer form, in the range 1-200000000.

【description】

stp cost the command to configure port path spending.

no stp cost the command to restore the default situation.

By default, the default value of cost depends on the physical interface rate: 20000 for 1000M interfaces by default; 2000 for 10G interfaces by default; 200000 for 10M interfaces by default.

【example】

#Configure the cost of port 0/0/1 to 3000.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp cost 3000

18.1.22 stp mcheck

【the command】

stp mcheck

【config-mode】

Port configuration mode

【parameter】

none

【description】

stp cost the command to trigger the mcheck function.

【example】

#Configure port 0/0/1 to trigger the mcheck function.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp mcheck

18.1.23 stp tcn-restricted

【the command】

stp tcn-restricted

no stp tcn-restricted

【config-mode】

Interface Configuration Mode

【parameter】

none

【description】

stp tcn-restricted the command enables the TCN BPDU propagation restriction function.

no stp tcn-restricted the command to restore the default situation.

By default, enable TCN BPDU propagation restriction is disabled.

【example】

#Configure port 0/0/1 to enable the TCN BPDU propagation restriction function.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp tcn-restricted

18.1.24 clear stp interface

【the command】

clear stp interface [ethernet *port-id* **]**

【config-mode】

Global configuration mode

【parameter】

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

clear stp interface the command to clear the STP statistics of a port.

【example】

#Configure to clear STP statistics for all ports.

Switch#configure terminal

Switch(config)#clear stp interface

18.2 STP/RSTPmonitoring and debugging the commands

18.2.1 show stp interface brief

【the command】

show stp interface brief

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show stp interface brief the command to view STP summary information.

【example】

#View STP summary information.

Switch(config)#show stp interface brief

Spanning-tree protocol: Enabled, spanning-tree mode: RSTP

STP info timeout factor: 3

TC protection: Enabled, interval: 10, threshold: 11

Bridge time: HelloTime 2s, MaxAge 20s, ForwardDelay 15s

Bridge ID: 32768-4418.4700.0000

Root Bridge: 32768-4418.4700.0000

Root Bridge time: HelloTime 2s, MaxAge 20s, ForwardDelay 15s

Path cost to root bridge: 0

Topo change times: 0

Port Protect: R-RootGuard, L-LoopGuard, B-BpduGuard, F-BpduFilter

---

Port	Cost	Priority	Protect	Role	State	Type
e0/0/2	20000	128.2	N/A	Root	Forwarding	P2P

show stp interface brief display field description

field	description
Spanning-tree protocol	Spanning Tree Enable State: Enabled, Disabled
Spanning-tree mode	Spanning Tree Protocol Mode: STP, RSTP, MSTP
STP info timeout factor	STP info timeout factor
TC protection	TC protection enable state, time period, threshold value
Bridge time	Bridge HelloTime, MaxAge, ForwardDelay information
Bridge ID	Bridge ID
Root Bridge	Root Bridge ID
Root Bridge time	Root Bridge HelloTime, MaxAge, ForwardDelay information
Path cost to root bridge	Path cost to root bridge
Topo change times	Topo change times
Port Protect	Description of marking
Port	port number

Cost	path overhead
Priority	port priority
Protect	Protection Configuration
Role	Interface Roles: Designated, Backup, Root, Alternate
State	Interface states: Discarding, Forwarding, Learning, Listening
Type	Link type: point-to-point, non-point-to-point, edge interface

18.2.2 show stp interface

【the command】

show stp interface [**ethernet** *port-id*]

【config-mode】

Arbitrary the command mode

【parameter】

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

show stp interface the command to view port STP details.

【example】

#View STP details for port 0/0/1.

Switch(config)#show stp interface ethernet 0/0/1

Spanning-tree protocol: Enabled, spanning-tree mode: RSTP

STP info timeout factor: 3

TC protection: Enabled, interval: 10, threshold: 11

Bridge time: HelloTime 2s, MaxAge 20s, ForwardDelay 15s

Bridge ID: 32768-4418.4700.0000

Root Bridge: 32768-4418.4700.0000

Path cost to root bridge: 0

Topo change times: 0

e0/0/1 STP state: LinkDown

Spanning-tree protocol: Enabled

remote loop detect is Disabled Port role: DesignatedPort

Port path cost: 300

Port priority: 0

Root guard: Disabled(block-port)

Loop guard: Enabled, port is not in loop-inconsistent state

Designated bridge: 32768-4418.4700.0000

Port is a non-edge port

Connected link type: not point-to-point

Max transmit limit: 12 BPDUs per HelloTime

Port time: HelloTime 2s, MaxAge 20s, ForwardDelay 15s, MessageAge 0

Rx info expired count: 0, last time:

Rx TC BPDU count: 0, last time:

TC Protection status: Normal

Tx BPDU: 0

TCN: 0, RST: 0, Config: 0

Rx BPDU: 0

TCN: 0, RST: 0, Config: 0

show stp interface ethernet 0/0/1 display field description

field	description
Spanning-tree protocol	Spanning Tree Enable State: Enabled, Disabled
Spanning-tree mode	Spanning Tree Protocol Mode: STP, RSTP, MSTP
STP info timeout factor	STP info timeout factor
TC protection	TC protection enable state, time period, threshold value
Bridge time	Bridge HelloTime, MaxAge, ForwardDelay information
Bridge ID	Bridge ID
Root Bridge	Root Bridge ID
Path cost to root bridge	Path cost to root bridge
Topo change times	Topo change times
e0/0/1 STP state	Interface STP Status：LinkDown、Blocking、Forwarding、Learning、Listening
Port role	Port role
Port path cost	Port path cost
Port priority	Port priority
Root guard	Root protection enable status and handling strategy

Loop guard	Ring protection enable state and operation state
Designated bridge	Designated bridge ID
Port is a non-edge port	Whether the port is an edge port: non-edge port, edge port
Connected link type	Port link type: point-to-point, shared link, auto
Max transmit limit	Maximum number of messages allowed to send BPDUs during Hello Time
Port time	Port Time Parameter Information
Rx info expired count	timeout counter
Rx TC BPDU count	Statistics of received TC messages
TC Protection status	TC Protection status
Tx BPDU	Sending BPDU statistics
Rx BPDU	Received BPDU statistics

18.3 MSTP configuration the commands

18.3.1 stp

【the command】

stp

no stp

【config-mode】

Global configuration mode

【parameter】

none

【description】

stp the command enables the STP function.

no stp the command disables the STP function.

By default, the global STP function is disabled and the port STP function is enabled.

【example】

#Enable the global STP function.

Switch#configure terminal

Switch(config)#stp

#Enable the STP function on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#stp

18.3.2 stp mode

【the command】

stp mode { stp | mstp | rstp }

【config-mode】

Global configuration mode

【parameter】

stp: Configure the spanning tree operating mode as STP mode.

mstp: Configure the spanning tree operating mode as MSTP mode.

rstp: Configure the spanning tree operating mode as RSTP mode.

【description】

stp mode the command configures the spanning tree operating mode.

no stp mode the command to restore the default situation.。

By default, the spanning tree operating mode is RSTP mode.

In STP mode, each port of the device will send STP BPDU messages outward, in RSTP mode, each port of the device will send RSTP BPDU messages outward, and in MSTP mode, each port of the device will send MSTP BPDU messages outward. MSTP is backward compatible with STP and RSTP, and RSTP is backward compatible with STP, i.e., a port working in MSTP mode will automatically migrate to work in the corresponding compatibility mode when it is found to be connected to a device running STP or RSTP, and a port working in RSTP mode will automatically migrate to work in the STP compatibility mode when it is found to be connected to a device running STP.

Note:

When Spanning Tree is globally enabled, modifications to the Spanning Tree operating mode will cause a restart of the protocol, which may result in a brief interruption of the network.

【example】

#Configure the spanning tree operating mode as MSTP mode.

Switch#configure terminal

Switch(config)#stp mode mstp

18.3.3 clear stp interface

【the command】

clear stp interface [ethernet *port-id* **]**

【config-mode】

Global configuration mode

【parameter】

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

clear stp interface the command to clear the STP statistics of a port.

【example】

#Configure to clear STP statistics for all ports.

Switch#configure terminal

Switch(config)#clear stp interface

18.3.4 mstp hello-time

【the command】

mstp hello-time *time-value*

no mstp hello-time

【config-mode】

Global configuration mode

【parameter】

time-value the time interval for sending BPDUs, in integer form, ranging from 1 to 10, in seconds.

【description】

mstp hello-time the command is used to configure the Hello Time of MSTP, i.e., the time interval for sending BPDUs.

no mstp hello-time the command to restore the default situation.

By default, the Hello Time for MSTP is 2 seconds.

Hello Time is used for MSTP to send configuration messages at regular intervals to maintain the stability of the spanning tree and to detect link failures. If the device does not receive BPDU messages for a certain period of time, the spanning tree is recalculated due to message timeout. When the device becomes the root device, use this the command to configure Hello Time to send BPDUs at regular intervals, while the non-root device adopts the Hello Time configured by the root device.

Note:

l max-age, hello-time and forward-time must satisfy the following relationship:

2 * (HelloTime + 1) <= MaxAge <= 2 * (ForwardDelay - 1)

【example】

#Configure the Hello Time value for MSTP to be 3 seconds.

Switch#configure terminal

Switch(config)#mstp hello-time 3

18.3.5 mstp forward-time

【the command】

mstp forward-time *time-value*

no mstp forward-time

【config-mode】

Global configuration mode

【parameter】

time-value: Forwarding delay time, in integer form, ranging from 4 to 30, in seconds.

【description】

mstp forward-time the command to configure the forwarding delay time for MSTP.

no mstp forward-time the command to restore the default situation.

By default, the MSTP forwarding delay is 15 secon

When the network topology changes, the spanning tree needs to be recalculated, and it takes some time for the new configuration messages to travel throughout the network. If the newly elected root interface and the designated interface forward the data immediately, it may cause a temporary path loopback. Therefore, before the interfaces forward the data again, they have to go through an intermediate state (learning), and the intermediate state can enter the forwarding state only after the forwarding delay time. Use this the command to configure the forwarding delay time to ensure that the new configuration message has been transmitted throughout the network. When the network topology changes infrequently, the delay time can be reduced appropriately, and vice versa.

Note:

l max-age, hello-time and forward-time must satisfy the following relationship:

2 * (HelloTime + 1) <= MaxAge <= 2 * (ForwardDelay - 1)

【example】

#Configure the forward-time value for MSTP to be 20 seconds.

Switch#configure terminal

Switch(config)#mstp forward-time 20

18.3.6 mstp max-age

【the command】

mstp max-age *time-value*

no mstp max-age

【config-mode】

Global configuration mode

【parameter】

time-value: Saves the time value, in integer form, in the range 6-40, in seconds.

【description】

mstp max-age the command configures the maximum retention time of BPDU configuration messages on the device.

no mstp max-age the command to restore the default situation.

By default, the max-age of MSTP is 20 seconds.

The BPDU configuration message is used for spanning tree calculation and maintenance.The message has a maximum retention time in the device, if the time is exceeded,the spanning tree will be recalculated. Too small a configured time may result in frequent recalculation of the spanning tree, while too large a time may result in the MSTP not being able to adapt to changes in the network topology in a timely manner.

Note:

l max-age, hello-time and forward-time must satisfy the following relationship:

2 * (HelloTime + 1) <= MaxAge <= 2 * (ForwardDelay - 1)

【example】

#Configure the max-age value for MSTP to be 30 seconds.

Switch#configure terminal

Switch(config)#mstp max-age 30

18.3.7 mstp time-factor

【the command】

mstp time-factor *time-factor-value*

no mstp time-factor

【config-mode】

Global configuration mode

【parameter】

time-factor-value: Timeout factor value, in integer form, configurable from 1-10.

【description】

mstp time-factor the command to configure the timeout factor.

no mstp time-factor the command to restore the default situation.

By default, the default timeout factor is equal to 3.

【example】

#Configure the timeout factor to be equal to 6.

Switch#configure terminal

Switch(config)#mstp time-factor 6

18.3.8 mstp max-hops

【the command】

mstp max-hops *max-hops-value*

no mstp max-hop

【config-mode】

Global configuration mode

【parameter】

max-hops-value: Maximum number of hops, in integer form, in the range 1-255.

【description】

mstp max-hops: Maximum number of hops for the command MST domain.

no mstp max-hops the command to restore the default situation.

By default, the max-hop of the MST domain is 20.

The maximum hop count of an MST domain limits the size of the MST domain, and the maximum hop count configured on the root of the domain will be used as the maximum hop count of this MST domain. Starting from the root bridge of the spanning tree within an MST domain, the hop count is reduced by 1 for each configuration message (i.e., BPDU) within the domain that isforwarded by a device, and the message is discarded if it has a hop count of 0. This limits the size of the MST domain by making devices that are outside the maximum hop count NONE method of participating in the spanning tree calculation.

【example】

#Configure the maximum number of hops for the MST domain as 30.

Switch#configure terminal

Switch(config)#mstp max-hops 30

18.3.9 mstp instance vlan

【the command】

mstp instance *instance-value* **vlan** *vlan-id*

no mstp instance *instance-value* **vlan** *vlan-id*

【config-mode】

Global configuration mode

【parameter】

instance-value: Spanning tree instance ID, in integer form, in the range 0-15.

vlan-id: VLAN ID, value range 1-4094. multiple VLAN IDs can be entered, non-consecutive VLAN IDs are separated by "," and consecutive VLAN IDs are separated by "-".

【description】

mstp instance vlan the command to configure the MSTP instance and VLAN mapping relationship.

no mstp instance vlan the command deletes the created MSTP instance and VLAN mapping relationship.

By default, the system automatically creates instance 0, and VLANs 1-4094 are mapped to instance 0.

A switched network can be divided into multiple MST domains, and an MST domain can include multiple independent MSTIs, a VLAN corresponds to an MSTI, and an MSTI corresponds to multiple VLANs. use this the command to configure the mapping relationship between MSTIs and VLANs, and if the configured MSTIs don't exist, then the MSTIs will be created automatically, and at the same time, the VLANs will be mapped. if the MSTIs exist, then the VLANs will be directly mapped to MSTIs. If the configured MSTI does not exist, the MSTI is created automatically and the VLANs are mapped at the same time.

In the spanning tree instance ID, 0 indicates a CIST instance, and other non-zero values indicate MSTI instances. When the mapping relationship between a VLAN and an MSTI instance is deleted, the VLAN is automatically mapped to instance 0.

The MST domain name, MSTP revision level, and VLAN mapping table together determine the MST domain to which the device belongs.

【example】

#Configure MSTP instance 1 to map VLAN 100.

Switch#configure terminal

Switch(config)#mstp instance 1 vlan 100

18.3.10 mstp instance priority

【the command】

mstp instance *instance-value* **priority** *priority-value*

no mstp instance *instance-value* **priority** *priority-value*

【config-mode】

Global configuration mode

【parameter】

instance-value: Spanning tree instance ID, in integer form, in the range 0-15.

priority-value: Priority, integer form, value range 0-61440, the next success is a multiple of 4096.

【description】

mstp instance priority the command to configure the bridge priority of the device in the specified spanning tree instance.

no mstp instance priority the command to restore the default situation.

By default, the device has a bridge priority of 32768 in every spanning tree instance.

【example】

#Configure the bridge priority of the device in spanning tree instance 1 to 4096.

Switch#configure terminal

Switch(config)#mstp instance 1 priority 4096

18.3.11 mstp instance port-priority

【the command】

mstp instance *instance-value* **port-priority** *priority-value*

no mstp instance *instance-value* **port-priority** *priority-value*

【config-mode】

Port configuration mode

【parameter】

instance-value: Spanning tree instance ID, in integer form, in the range 0-15.

priority-value: Priority, integer form, value range 0-240.

【description】

mstp instance port-priority the command to configure the priority of a port in a specified spanning tree instance.

no mstp instance port-priority the command to restore the default situation.

By default, ports have a priority of 128 in every spanning tree instance.

【example】

#Configure the priority in port 0/0/1 spanning tree instance 1 to be 128.

Switch#configure terminal

Switch(config)#mstp instance 1 port-priority 128

18.3.12 mstp instance cost

【the command】

mstp instance *instance-value* **cost** *cost-value*

no mstp instance *instance-value* **cost** *cost-value*

【config-mode】

Port configuration mode

【parameter】

instance-value: Spanning tree instance ID, in integer form, in the range 0-15.

cost-value: Path overhead, in integer form, in the range 1-200000000.

【description】

mstp instance cost the command to configure the path overhead of a port in a specified spanning tree instance.

no mstp instance cost the command to restore the default situation.

By default, the port's path overhead will be set automatically based on the port rate.

【example】

#Configure port 0/0/1 to have a path overhead of 1000 in spanning tree instance 1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp instance 1 cost 1000

18.3.13 mstp external cost

【the command】

mstp external cost *cost-value*

no mstp external cost

【config-mode】

Port configuration mode

【parameter】

cost-value: Path overhead, in integer form, in the range 1-200000000.

【description】

mstp external cost the command to configure the port's external path overhead.

no mstp external cost the command to restore the default situation.

By default, the port's path overhead will be set automatically based on the port rate.

【example】

#Configure the external path overhead for port 0/0/1 to 1000.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp external cost 1000

18.3.14 mstp revision

【the command】

mstp revision *value*

no mstp revision

【config-mode】

Global configuration mode

【parameter】

value: Revision level, integer form, range 1-65535.。

【description】

mstp revision the command to configure the MSTP revision level.

no mstp revision the command to restore the default situation.

By default, the revision level is 0.

【example】

#Configure the system revision level to 100.

Switch#configure terminal

Switch(config)#mstp revision 100

18.3.15 mstp region-name

【the command】

mstp region-name *value*

no mstp region-name

【config-mode】

Global configuration mode

【parameter】

value: MST domain name, in string form, supports up to 32 characters.

【description】

mstp region-name the command to configure the domain name.

no mstp region-name the command to delete the domain name.

【example】

#Configure the domain name as name.

Switch#configure terminal

Switch(config)#mstp region-name name

18.3.16 mstp config-digest-snooping

【the command】

mstp config-digest-snooping

no mstp config-digest-snooping

【config-mode】

Port configuration mode

【parameter】

none

【description】

mstp config-digest-snooping the command enables the summary listening function.

no mstp config-digest-snooping the command to restore the default situation.

By default, the summary listening function is disabled.

【example】

#Enable summary listening on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp config-digest-snooping

18.3.17 mstp enable instance

【the command】

mstp enable instance *instance-value*

【config-mode】

Global configuration mode

【parameter】

instance-value: Spanning tree instance ID, in integer form, in the range 1-15.

【description】

mstp enable instance the command enables the spanning tree instance function.

By default, all instances are enabled.

【example】

#Enable MSTP instance 1.

Switch#configure terminal

Switch(config)#mstp enable instance 1

18.3.18 mstp disable instance

【the command】

mstp disable instance *instance-value*

【config-mode】

Global configuration mode

【parameter】

instance-value: Spanning tree instance ID, in integer form, in the range 1-15.

【description】

mstp disable instance the command disables the enable spanning tree instance function.

By default, all instances are enabled.

【example】

#Disable enable MSTP instance 1.

Switch#configure terminal

Switch(config)#mstp disable instance 1

18.3.19 mstp portfast

【the command】

mstp portfast { autoedge | edgeport | disable }

no mstp portfast

【config-mode】

Port configuration mode

【parameter】

autoedge: Indicates that the port is automatically detected as an edge port.

edgeport: Indicates that the port is forced to be an edge port.

disable: Indicates that the port is forced to be a non-edge port.

【description】

mstp portfast the command to configure the physical interface as an edge port.

no mstp portfast the command to restore the default situation.

By default, all ports are autoedg.

An edge port is a port that is directly connected to a user. Edge ports do not create temporary loops when the network topology changes, so if a port is configured as an edge port, the port can quickly enter the forwarding state.

【example】

#Configure port 0/0/1 as an edge port.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp portfast edgeport

18.3.20 mstp link-type

【the command】

mstp link-type { auto | point-to-point | shared }

no mstp link-type

【config-mode】

Port configuration mode

【parameter】

auto: Indicates that the link connected to this port is automatically detected as a point-to-point link.

point-to-point: Indicates that the link to the current port is a point-to-point link.

shared: Indicates that the link connected to the current port is not a point-to-point link and is a shared link.

【description】

mstp link-type the command to configure the link type of the port.

no mstp link-type the command to restore the default situation.

By default, the link type is configured as auto. the device configures the link type of a port according to the duplex state. Full-duplex ports are considered point-to-point links and half-duplex ports are recognized as shared links.

Note:

If a port is configured to connect to a point-to-point link, but the physical link to which the port is actually connected is not a point-to-point link, it is possible to introduce temporary loops

【example】

#Configure the link type of port 0/0/1 as a point-to-point link.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp link-type point-to-point

18.3.21 mstp bpdu-filter

【the command】

mstp bpdu-filter

no mstp bpdu-filter

【config-mode】

Global configuration mode/Port configuration mode

【parameter】

none

【description】

mstp bpdu-filter the command is used to configure the enable BPDU filtering function.

no mstp bpdu-filter the command to restore the default situation.

By default, BPDU filtering is disabled.

Use this the command to enable BPDU filtering. It takes effect only for edge ports, and will not take effect for other ports.

When bpdu-filter is enabled under the port, the edge port will not process and send BPDU messages.

When bpdu-filter is globally enabled, the edge port does not actively send bpdu, but participates in the stp calculation according to the normal process after receiving bpdu.

When bpdu-filter is enabled both globally and on the port, edge ports with bpdu-filter enabled follow the port function, and edge ports without bpdu-filter enabled follow the global function.

【example】

#Enable BPDU filtering on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp bpdu-filter

18.3.22 mstp bpdu-guard

【the command】

mstp bpdu-guard

no mstp bpdu-guard

【config-mode】

Port configuration mode

【parameter】

none

【description】

mstp bpdu-guard the command is used to configure the enable BPDU protection function.

no mstp bpdu-guard the command to restore the default situation.

By default, BPDU protection is disabled.

The BPDU Guard function of a port takes effect only on edge ports. For the ports that have been configured with the edge port attribute but become non-edge ports again because they receive BPDU packets from other ports, the BPDU Guard function takes effect only on the edge ports. After the BPDU Guard function is enabled, if the edge port receives BPDU messages, it will be down, and you need to restart the port manually to recover.

Note:

If BPDU-filter and BPDU-Guard are both enabled, the BPDU-filter function takes precedence.

【example】

#Enable BPDU protection on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp bpdu-guard

18.3.23 mstp loop-guard

【the command】

mstp loop-guard

no mstp loop-guard

【config-mode】

Port configuration mode

【parameter】

none

【description】

mstp loop-guard the command is used to configure the enable port ring protection function.

no mstp loop-guard the command to restore the default situation.

By default, enable port ring protection is disabled.

Use this the command to enable the Loop guard function. If the spanning tree information stored on a port is aged because the port does not receive BPDU messages from the upstream device, causing the spanning tree to be recalculated, the port will be set to the Discarding state when recalculating the role of the port and will not participate in the spanning tree calculation. If the instance on the port receives BPDU messages again, it participates in the spanning tree calculation again.

Note:

l The function of ring protection is antithetical to the function of link backup, i.e., ring protection avoids loops at the expense of losing the link backup function.

2 Root Guard and Loop Guard cannot be used simultaneously on the same port.

【example】

#Enable ring protection on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp loop-guard

18.3.24 mstp root-guard

【the command】

mstp root-guard

no mstp root-guard

【config-mode】

Port configuration mode

【parameter】

none

【description】

mstp root-guard the command is used to configure the enable port root protection function.

no mstp root-guard the command to restore the default situation.

By default, port root protection is disabled.

Use this the command to enable the port Root Guard function. The port role on all instances of a port with the Root Guard function enabled can only remain as the specified port. Once the port receives a better BPDU configuration message, the port state will be set to Discarding state, and you need to manually reboot the port to restore it.

Note:

Root Guard and Loop Guard cannot be used simultaneously on the same port.

【example】

#Enable root protection on port 0/0/1.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp root-guard

18.3.25 mstp root-guard action

【the command】

mstp root-guard action { block-port | drop-bpdu }

【config-mode】

Global configuration mode

【parameter】

block-port: Indicates a blocked port.

drop-bpdu: Indicates that the BPDU message is discarded.

【description】

mstp root-guard action the command to configure the processing behavior of Root Guard.

By default, the processing behavior is block-port.

【example】

#Configure the processing behavior of the Root Guard feature as drop-bpdu.

Switch#configure terminal

Switch(config)#mstp root-guard action drop-bpdu

18.3.26 mstp flap-guard

【the command】

mstp flap-guard

no mstp flap-guard

【config-mode】

Global configuration mode

【parameter】

none

【description】

mstp flap-guard the command is used to configure the enable flap protection function.

no mstp flap-guard the command user to restore the default situation.

By default, flap protection is disabled.

【example】

#Enable the flap protection function.

Switch#configure terminal

Switch(config)#mstp flap-guard

18.3.27 mstp flap-guard max-flaps

【the command】

mstp flap-guard max-flaps *flaps-value* **time** *period-value*

no mstp flap-guard max-flaps

【config-mode】

Global configuration mode

【parameter】

flaps-value: Maximum number of times, in integer form, in the range 1-100.

period-value: Detection period, in integer form, ranging from 1 to 60 in seconds.

【description】

mstp flap-guard max-flaps the command configures the flap guard probe frequency parameter.

no mstp flap-guard max-flaps the command user to restore the default situation.

By default, the Flap Guard function is disabled. After enabling, the default detection frequency is 5 times of root port color change within 10 seconds, then it will enter the Flap Guard state.

【example】

#Configure the Flap Guard state to be entered if six root port role changes occur within 20 seconds.

Switch#configure terminal

Switch(config)#mstp flap-guard max-flaps 6 time 20

18.3.28 mstp flap-guard recovery-time

【the command】

mstp flap-guard recovery-time *value*

no mstp flap-guard recovery-time

【config-mode】

Global configuration mode

【parameter】

value: Takes a value, in integer form, in the range 30-1000, in seconds.

【description】

mstp flap-guard recovery-time the command configures the flap guard recovery time.

no mstp flap-guard recovery-time the command user to restore the default situation.

By default, the recovery time is 30 seconds.

【example】

#Configure the flap guard recovery time of 50 seconds.

Switch#configure terminal

Switch(config)#mstp flap-guard recovery-time 50

18.3.29 mstp tc-protection

【the command】

mstp tc-protection

no mstp tc-protection

【config-mode】

Global configuration mode

【parameter】

none

【description】

mstp tc-protection the command enables the TC BPDU attack protection function.

no mstp tc-protection the command user to restore the default situation.

By default, enable TC BPDU attack protection is disabled.

【example】

#Enable the TC BPDU attack protection function.

Switch#configure terminal

Switch(config)#mstp tc-protection

18.3.30 mstp tc-protection interval

【the command】

mstp tc-protection interval *interval-value*

no mstp tc-protection interval

【config-mode】

Global configuration mode

【parameter】

interval-value: Send cycle value, in integer form, in the range 1-255.

【description】

mstp tc-protection interval the command configures the time period for processing TC BPDU messages.

no mstp tc-protection interval the command user to restore the default situation.

By default, the time period for processing TC BPDU messages is 10 seconds.

【example】

#Configure the TC BPDU time period as 30s.

Switch#configure terminal

Switch(config)#mstp tc-protection interval 30

18.3.31 mstp tc-protection threshold

【the command】

mstp tc-protection threshold *interval-value*

no mstp tc-protection threshold

【config-mode】

Global configuration mode

【parameter】

interval-value: Threshold value, in integer form, in the range 1-255.

【description】

mstp tc-protection threshold the command configures the maximum number of TC BPDU messages to be processed per unit time period.

no mstp tc-protection threshold the command user to restore the default situation.

By default, the maximum number of times that the device refreshes the forwarding address table entry immediately after receiving a TC BPDU in a unit of time is 6.

【example】

#Configure the maximum number of times to process TC BPDU messages as two.

Switch#configure terminal

Switch(config)#mstp tc-protection threshold 2

18.3.32 mstp mcheck

【the command】

mstp mcheck

【config-mode】

Port configuration mode

【parameter】

none

【description】

mstp mcheck the command to trigger the mcheck function.

Executing this the command is valid only when the working mode of spanning tree is MSTP & RSTP mode.

Only valid for a single time, the command will not be decompiled and cannot be saved.

【example】

#Port 0/0/1 triggers mcheck.

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#mstp mcheck

18.4 MSTP monitoring and debugging the commands

18.4.1 show mstp instance brief

【the command】

show mstp instance brief [*instance-value*]

【config-mode】

Arbitrary the command mode

【parameter】

instance-value: Spanning tree instance ID, in integer form, in the range 1-15.

【description】

show mstp instance brief the commands view MSTP configuration and status information.

【example】

#View MSTP configuration and status information.

Switch(config)#show mstp instance brief

Current spanning tree protocol is MSTP

Spanning tree protocol is enable

Received information time factor is 3

TC protection is enable, interval is 10, threshold is 6

Flap guard is disable, max count 5, detect perid 10 s, recovery period 30 s

MSTP Instance 0 vlans mapped:1-99,101-4094

Bridge ID 32768-00e0.5317.e1e4

CIST root 32768-00e0.5317.e1e4

Region root 32768-00e0.5317.e1e4

Bridge time HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20

Cist Root time HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20

External rpc: 0, Internal rpc: 0

PortID	Role	Sts	ExternalCost	InternalCost	Prio.Nbr	Type
GE0/0/2	Design	FWD	20000	20000	128.2	P2P Edge

show mstp instance brief display field description

field	description
Spanning-tree protocol	Spanning Tree Enable State: Enabled, Disabled
Spanning-tree mode	Spanning Tree Protocol Mode: STP, RSTP, MSTP
STP info timeout factor	STP info timeout factor
TC protection	TC protection enable state, time period, threshold value
Flap guard	Flap protection function enable status, maximum number of times, time period, recovery time
Bridge ID	Bridge ID
CIST root	CIST root Bridge
Region root	Region root Bridge
Bridge time	Bridge Time Parameter Information
Cist Root time	CIST Roots Bridge Time Parameter Information

PortID	Port number
Role	Port role：Designated、Backup、Root、Alternate
Sts	Port state：Discarding、Forwarding、Learning、Listening
ExternalCost	External path cost
InternalCost	Internal path cost
Prio.Nbr	Port priority
Type	Link type: point-to-point, non-point-to-point, edge interface

18.4.2 show mstp instance interface

【the command】

show mstp instance *instance-value* **interface [brief] [ethernet** *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

instance-value: Instance ID, in integer form, in the range 0-15.

brief: Indicates to view brief information.

port-id: Port number, integer form, the value range is determined by the device model, format such as 0/0/1.

【description】

show mstp instance interface the command to view port MSTP information.

【example】

#View port 0/0/1 MSTP details.

```
Switch(config)#show mstp instance 0 interface ethernet 0/0/1
Current spanning tree protocol is MSTP
  Spanning tree protocol is enable
  Received information time factor is 3
  TC protection is enable, interval is 10, threshold is 6
  Flap guard is disable, max count 5, detect perid 10 s, recovery period 30 s
  Bridge id is 32768-00e0.5317.e1e4
  Cist root is 32768-00e0.5317.e1e4,root port is NULL
  Region root is 32768-00e0.5317.e1e4,root port is NULL
  Bridge time:HelloTime 2,MaxAge 20,ForwardDelay 15,MaxHops 20
  Cist Root time:HelloTime 2,MaxAge 20,ForwardDelay 15,RemainingHops 20
  External root path cost is 0,internal root path cost is 0

Port GE0/0/1 of instance 0 is Down
  Port role is disabledPort, priority is 128
  Port external path cost is 200000,internal path cost is 200000
  Root guard disable and port is not in root-inconsistent state
  Loop guard disable and port is not in loop-inconsistent state
  Designated bridge is 32768-00e0.5317.e1e4,designated port is GE0/0/1
  Port is a(n) edge port,link type is non-point-to-point
  Port time:HelloTime 2,MaxAge 20,FwdDelay 15,MsgAge 0,RemainingHops 20
  Received TC flag BPDU count:0; last time:
  TC Protection status: Normal
  Received information expired count:0; last time:
  Received BPDUs:TCN 0,RST 0,Config BPDU 0
```

Transmitted BPDUs:TCN 0,RST 0,Config BPDU 0

show mstp instance 0 interface ethernet 0/0/1 display field description

field	description
Port time	Time parameter information saved by the port
Received TC flag BPDU count	TC BPDU message statistics
last time	Time of last TC BPDU message received
TC Protection status	TC Anti-Attack Detection Status
Received information expired count	Receive Timeout BPDU Message Statistics
last time	Last time a timeout BPDU message was received
Received BPDUs	Statistics of received BPDU messages
Transmitted BPDUs	Statistics of sent BPDU messages

18.4.3 show mstp config-id

【the command】

show mstp config-id

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show mstp config-id the command to view the configuration information of an MSTP domain.

【example】

#View configuration information for the MSTP domain.

Switch(config)#show mstp config-id

Revision level : 0

Config name :

instance 1 : 100

instance 2 :

instance 3 :

instance 4 :

instance 5 :

instance 6 :

instance 7 :

instance 8 :

instance 9 :

instance 10 :

instance 11 :

instance 12 :

instance 13 :

instance 14 :

instance 15 :

Other VLANs are mapped to Instance 0

show mstp config-id display field description

field	description
Revision level	domain revision level
Config name	domain name
instance 1-15	Each instance maps to a VLAN

18.4.4 show mstp disabled-instance

【the command】

show mstp disabled-instance

【config-mode】

Arbitrary the command mode

【parameter】

none

【description】

show mstp disabled-instance the command to view disabled instance information.

【example】

#Viewing Disabled Instance Information

Switch(config)# show mstp disabled-instance

Instance-Disabled : 11

show mstp disabled-instance display field description

field	description

Instance-Disabled	Disabled instance ID

Chapter 19 Loopback-detection

19.1 loopback-detection configuration the commands

19.1.1 loopback-detection

【the command】

loopback-detection

no loopback-detection

【config-mode】

Global configuration mode/Port configuration mode

【parameter】

none

【description】

loopback-detection the command enables the loopback detection function.

no loopback-detection the command disables the enable loopback detection function.

By default, the loopback detection function is not enable

Note:

To configure loopback detection, the global loopback detection control switch must be enabled before the Ethernet interface's loopback detection configuration can take effect.

【example】

#Enable global loopback detection

Switch#configure terminal

Switch(config)#loopback-detection

#Enable loopback detection on port 0/0/1

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#loopback-detection

19.1.2 loopback-detection interface

【the command】

loopback-detection interface [ethernet *port-id* **]**

no loopback-detection interface [ethernet *port-id* **]**

【config-mode】

Global configuration mode

【parameter】

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

loopback-detection interface the command configures the loopback detection function of the port.

no loopback-detection interface the command disables the loopback detection function of the configured port.

By default, the port loopback detection function is not enabled.

【example】

#Configure loopback detection for all ports.

Switch#configure terminal

Switch(config)#loopback-detection interface

19.1.3 loopback-detection action

【the command】

loopback-detection action{ discarding | shutdown }

【config-mode】

Global configuration mode

【parameter】

discarding: Indicates that the port is blocked when a loopback is detected.

shutdown: Indicates that the port is down after a loopback is detected.

【description】

loopback-detection action the command is used to configure the processing behavior when a loopback is detected.

By default, the processing behavior is discarding.

【example】

#Configure the handling behavior for detecting a loopback as shutdown.

Switch#configure terminal

Switch(config)#loopback-detection action shutdown

19.1.4 loopback-detection interval-time

【the command】

loopback-detection interval-time *interval-time-value*

【config-mode】

Global configuration mode

【parameter】

interval-time-value: Loopback detection period, integer form, value range 5-300 in seconds.

【description】

loopback-detection interval-time the command configures the loopback detection send packet period.

By default, the detection period is 5s.

【example】

#Configure the loopback detection period as 300s.

Switch#configure terminal

Switch(config)#loopback-detection interval-time 300

19.2 loopback-detection monitoring and debugging the commands

19.2.1 show loopback-detection

【the command】

show loopback-detection [ethernet *port-id* **]**

【config-mode】

Arbitrary the command mode

【parameter】

port-id: Port number, the value range is determined by the device model, such as 0/0/1.

【description】

show loopback-detection the command is used to view the loopback detection configuration and detection information.

【example】

#View loopback detection information for port 0/0/1.

Switch(config)#show loopback-detection ethernet 0/0/1

LB-Detect:Disable

Loopback-detection action is Shutdown

The interval time is 300 seconds

The recovery time of the discarding action is 900 seconds

Port Information:

port loopback status

e0/0/1 Enable Normal

show loopback-detection ethernet 0/0/1 display field description

field	description
LB-Detect	global enable state
Loopback-detection action	Loopback-detection action
The interval time	Loopback-detection interval time
The recovery time	Loopback-detection recovery time
Port	Port number
Loopback	Port loopback-detection enable state
Status	Port loopback-detection results

Chapter 20 ARP

20.1 ARP Configuration Commands

20.1.1 arp ip-address mac-address

【command】

arp *ip-address mac-address* **[vlan** *vlan-vid* **| ethernet** *port-id* **]**

no arp *ip-address*

【config-mode】

Global configuration mode

【parameter】

ip-address:ip address,dotted decimal format,such as:192.168.1.1.

mac-address:mac address, hexadecimal format,such as:00:00:11:22:33:44.

vlan-vid:vlan id,decimal integer format,value range 1-4094.

port-id:port number,the format is:device number/slot number/port number,such as:0/0/1.

【description】

arp *ip-address mac-address* the command is used to configure short static ARP table entries.

arp *ip-address mac-address* [**vlan** *vlan-vid* **ethernet** *port-id*] the command is used to configure long static ARP table entries.

no arp *ip-address* The command is used to delete specified ARP table entries.

When configuring static ARP table entries,the IP address must be in the same network segment as the IP of the VLAN interface corresponding to the VLAN,otherwise the addition will not be successful.

The short static ARP table entry cannot be directly used for message forwarding,if the device receives the source IP address and source MAC address in the ARP request packet that are the same as the IP address and MAC address in the configured short static ARP,the ARP table entry will be automatically supplemented and can then be used for IP packet forwarding.

【example】

#Configure a long static ARP table entry,the MAC address in this table entry is 00:00:11:11:11:11:11,VLAN id is 1,IP address is 192.168.1.2.

Switch#configure terminal

Switch(config)#arp 192.168.1.2 00:00:11:11:11:11 vlan 1 ethernet 0/0/1

20.1.2 arp aging-time

【command】

arp aging-time *time-value*

no arp aging-time

【config-mode】

Global configuration mode

【parameter】

time-value:aging time,value range 3-2880 minutes,default is 20 minutes.

【description】

arp aging-time The command is used to configure dynamic ARP table Fields aging time.

no arp aging-time The command is used to restore ARP aging time as default.

【example】

#Configure dynamic ARP table entry aging time of 10 minutes.

Switch#configure terminal

Switch(config)#arp aging-time 10

20.1.3 arp bind dynamic

【command】

arp bind dynamic { *ip-address* | **all** }

【config-mode】

Global configuration mode

【parameter】

ip-address:ip address,dotted decimal format,such as:192.168.1.1.

【description】

arp bind dynamic *ip-address* the command is used to bind specified dynamic ARP table entries to static ARP table entries.

arp bind dynamic all the command is used to bind all dynamic ARP table entries to static table entries.

【example】

#Configure binding all dynamic ARP table Fieldss to static ARP table Fieldss.

Switch#configure terminal

Switch(config)#arp bind dynamic all

20.1.4 no arp

【command】

no arp { all | dynamic | static }

【config-mode】

Global configuration mode

【parameter】

None

【description】

no arp all the command is used to delete all ARP table entries.

no arp dynamic the command is used to delete all dynamic ARP table entries.

no arp static the command is used to delete all static ARP table entries.

【example】

#Delete all dynamic ARP table entries.

Switch#configure terminal

Switch(config)#no arp all

All the arp entries will be deleted?

Please confirm: (y/n) [n]y

20.2 ARP Monitoring and Debug Commands

20.2.1 show arp

【command】

show arp { *ip-address [mask]* | *mac-address* **}**

【config-mode】

Any configuration mode

【parameter】

ip-address:ip address,dotted decimal format,such as:192.168.1.1.

mask:subnet mask,decimal format,such as:255.255.255.0.

mac-address:mac address,hexadecimal format,such as:00:00:11:22:33:44.

【description】

show arp *ip-address* [mask] The command is used to view the ARP table entries for the specified IP address.

show arp *mac-address* The command is used to view the ARP table entries for the specified MAC address.

【example】

#View the ARP table entry with IP = 192.168.1.28,mask = 255.255.255.0.

Switch#configure terminal

Switch(config)#show arp 192.168.1.28 255.255.255.0

Information of ARP

IpAddress	Mac_Address	Vlan	Port	Type	Status	ExpireTime
192.168.1.28	44:18:47:28:28:28	1	LAG1	dynamic	REACHABLE	1177 sec

Total entries: 1, Printed entries: 1

show arp fields description

Fields	Description
IpAddress	IP address
Mac_Address	MAC address
Vlan	VLAN ID
Port	Port number
Type	Type:dynamic、static、permanent、blackhole
Status	Status
ExpireTime	Remaining aging time
Total entries	Total number of table entries
Printed entries	Number of table Fieldss displayed

20.2.2 show arp { all | dynamic | static }

【command】

show arp { all | dynamic | static }

【config-mode】

Any configuration mode

【parameter】

None

【description】

show arp all The command is used to view all ARP table entries.

show arp dynamic The command is used to view all dynamic ARP table entries.

show arp static The command is used to view all static ARP table entries.

【example】

#View all dynamic ARP table entries.

Switch#configure terminal

Switch(config)#show arp dynamic

Information of ARP

IpAddress	Mac_Address	Vlan	Port	Type	Status	ExpireTime
192.168.1.28	44:18:47:28:28:28	1	LAG1	dynamic	REACHABLE	317 sec
192.168.1.111	00:26:38:b2:d5:a6	1	0/0/18	dynamic	REACHABLE	1183 sec

Total entries: 2, Printed entries: 2

show arp dynamic fields description

Fields	Description
IpAddress	IP address
Mac_Address	MAC address
Vlan	VLAN ID
Port	Port number
Type	Type:dynamic

Status	Status
ExpireTime	Remaining aging time
Total entries	Total number of table entries
Printed entries	Number of table Fieldss displayed

20.2.3 show arp aging-time

【command】

show arp aging-time

【config-mode】

Any configuration mode

【parameter】

None

【description】

show arp aging-time The command is used to view ARP table Fields aging time.

【example】

#View ARP table Fields aging time.

Switch#configure terminal

Switch(config)#show arp aging-time

Information of arp aging-time

ARP ageing-time: 10 minutes

20.2.4 debug arp

【command】

debug arp

no debug arp

【config-mode】

Global configuration mode

【parameter】

None

【description】

debug arp The command is used to open the ARP debug information.

no debug arp The command is used to close the ARP debug information.

By default,the ARP debugging switch is off.

【example】

#Open the ARP debug information.

switch#configure terminal

switch(config)#debug arp

Chapter 21 ARP Proxy

21.1 ARP Proxy Configuration Commands

21.1.1 arp-proxy

【command】

arp-proxy

no arp-proxy

【config-mode】

VLAN/SuperVLAN interface configuration mode

【parameter】

None

【description】

arp-proxy The command is used to enable ARP proxy function.

no arp-proxy The command is used to restore default configuration.

By default,disable enabling ARP proxy function.

【example】

#Enable the ARP proxy function of VLAN interface 1.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#arp-proxy

21.1.2 local-arp-proxy

【command】

local-arp-proxy

no local-arp-proxy

【config-mode】

SuperVLAN interface configuration mode

【parameter】

None

【description】

local-arp-proxy The command is used to enable local ARP proxy function.

no local-arp-proxy The command is used to restore default configuration.

By default,disable enabling local ARP proxy function.

【example】

#Enable the local ARP proxy funtion of SuperVLAN interface 1.

Switch#configure terminal

Switch(config)#interface supervlan-interface 1

Switch(config-if-superVLANInterface-1)#local-arp-proxy

21.2 ARP Proxy Monitoring and Debug Commands

21.2.1 show arp-proxy

【command】

show arp-proxy

【config-mode】

Any configuration mode

【parameter】

None

【description】

show arp-proxy The command is used to view the ARP proxy configuration information.

【example】

#View the ARP proxy configuration information.

Switch#configure terminal

Switch(config)#show arp-proxy

Information of arp-proxy

Subnet Name : Enable

VLAN-IF1 : FALSE

superVLAN-IF1 : FALSE

Total entries:2

show arp-proxy fields description

Fields	Description
Subnet Name	VLAN/SuperVLAN interface name
Enable	State of enable:FALSE、TRUE
Total entries	Total number of table entries

21.2.2 show local-arp-proxy

【command】

show local-arp-proxy

【config-mode】

Any configuration mode

【parameter】

None

【description】

show local-arp-proxy The command is used to view the local ARP proxy configuration information.

【example】

#View the local ARP proxy configuration information.

Switch#configure terminal

Switch(config)#show local-arp-proxy

Information of local-arp-proxy

Subnet Name : Enable

VLAN-IF1 : FALSE

superVLAN-IF1 : FALSE

Total entries:2

show local-arp-proxy fields description

Fields	Description
Subnet Name	VLAN/superVLAN interface name
Enable	State of enable:FALSE、TRUE
Total entries	Total number of table entries

Chapter 22 NDP

22.1 NDP Configuration Commands

22.1.1 ipv6 nd ns reachable-time

【command】

ipv6 nd ns reachable-time *time-value*

no nd ns reachable-time

【config-mode】

VLAN/SuperVLAN interface configuration mode

【parameter】

time-value:reachable state time,the value ranges from 1 to 3600,default value is 30,in seconds.

【description】

ipv6 nd ns reachable-time *time-value* The command is used to configure neighbor reachable state time.

no nd ns reachable-time The command is used to restore default configuration.

By default,neighbor reachable state time is 30 seconds.

【example】

#Configure neighbor reachable state time to 100.

Switch#configure terminal

Switch(config)#ipv6 nd reachable-time 100

22.1.2 ipv6 nd ns retrans-time

【command】

ipv6 nd ns retrans-time *time-value*

no ipv6 nd ns retrans-time

【config-mode】

VLAN/SuperVLAN interface configuration mode

【parameter】

time-value:time interval,decimal integer format,value range 1-3600,unit seconds.

【description】

ipv6 nd ns retrans-time *time-value* The command is used to configure send NS message period.

no ipv6 nd ns retrans-time The command is used to restore default configuration.

By default,time period for sending NS is 1 second.

【example】

#Configure the time period for sending NS to 2 second.

Switch#configure terminal

Switch(config)#ipv6 nd ns retrans-time 2

22.1.3 ipv6 neighbors max-learning-num

【command】

ipv6 neighbors max-learning-num *num-value*

no ipv6 neighbors max-learning-num

【config-mode】

Global configuration mode

【parameter】

num-value:the number of neighbors,decimal integer format,value range 1-2048.

【description】

ipv6 neighbors max-learning-num *num-value* The command is used to limit the number of learning neighbors.

no ipv6 neighbors max-learning-num The command is used to restore default configuration.

By default,the maximum number of learning neighbors is 2048.

【example】

#Configure the number of neighbor learning to 100.

Switch#configure terminal

Switch(config)#ipv6 neighbors max-learning-num 100

22.1.4 ipv6 neighbor ipv6-address mac-address

【command】

ipv6 neighbor *ipv6-address mac-address* **[vlan** *vlan-vid* **ethernet** *port-id* **]**

no ipv6 neighbor *ipv6-address*

【config-mode】

Global configuration mode

【parameter】

ipv6-address:ipv6 address,decimal hexadecimal format,such as 2000::1.

mac-address:mac address,decimal hexadecimal format,such as 00:00:11:22:33:44.

vlan-vid:vlan id,decimal integer format,value range 1-4094.

port-id:port number,the format is:device number/slot number/port number,such as 0/0/1.

【description】

ipv6 neighbor *ipv6-address mac-address* The command is used to configure short static neighbor table Fieldss.

ipv6 neighbor *ipv6-address mac-address* **vlan** *vlan-vid* **ethernet** *port-id* The command is used to configure long static neighbor table Fieldss.

no ipv6 neighbor *ipv6-address* The command is used to delete the specified neighbor table entry.

When configuring static neighbor table entries,IPv6 address need to be on the same network segment as the VLAN interface corresponding to the VLAN,otherwise the addition is unsuccessful.

Short static neighbor table entries cannot be used for message forwarding directly. If the device receives the same source IPv6 address and source MAC address in the neighbor request message as the configured short static neighbor IPv6 address and MAC address, the neighbor table entries are automatically complemented and then can be used for packet forwarding..

【example】

#Configure a long static neighbor table entry with MAC 00:00:11:11:11:11, VLAN number 1, IPv6 2000::1.

Switch#configure terminal

Switch(config)#ipv6 neighbor 2000::1 00:00:11:01:01:01 vlan 1 ethernet 0/0/1

22.1.5 no ipv6 neighbor

【command】

no ipv6 neighbor { **all** | **dynamic** | **static** | *ipv6-address*}

【config-mode】

Global configuration mode

【parameter】

None

【description】

no ipv6 neighbor The command is used to delete all neighbor table entries.

no ipv6 neighbor dynamic The command is used to delete all dynamic neighbor table entries.

no ipv6 neighbor static The command is used to delete all static neighbor table entries.

【example】

#Delete all neighbor table entries.

Switch#configure terminal

Switch(config)#no ipv6 neighbor all

All the neighbor cache entries will be deleted?

Please confirm: (y/n) [n]y

22.2 NDP Monitoring and Debug Commands

22.2.1 show ipv6 neighbors

【command】

show ipv6 neighbors { *ipv6-address* | **mac** *mac-address* }

【config-mode】

Any configuration mode

【parameter】

ipv6-address:ipv6 address,decimal hexadecimal format,such as 2000::1.

mac-address:mac address,decimal hexadecimal format,such as 00:00:11:22:33:44.

【description】

show ipv6 neighbors *ipv6-address* The command is used to view the neighbor table entries for the specified IPV6 address.

show ipv6 neighbors mac *mac-address* The command is used to view the neighbor table entries for the specified MAC address.

【example】

#View neighbor table entries with a specified IPv6 address of 2000:: 1.

Switch#configure terminal

Switch(config)#show ipv6 neighbors 2000::1

Information of neighbors

IpAddress	Mac_Address	Vlan	Port	Type	Status	ExpireTime
2000::1	00:00:11:01:01:01	1	0/0/1	static	PERMANENT	--

Total entries: 1, Printed entries: 1

show ipv6 neighbors display fields description information

Fields	Description
IpAddress	IP address

Mac_Address	MAC address
Vlan	VLAN ID
Port	Port ID
Type	Type:dynamic、static
Status	status
ExpireTime	Remaining aging time
Total entries	Total number of table entries
Printed entries	Number of displays

22.2.2 show ipv6 neighbors { all | dynamic | static }

【command】

show ipv6 neighbors { all | dynamic | static }

【config-mode】

Any configuration mode

【parameter】

None

【description】

show ipv6 neighbors all The command is used to view all neighbor table entries.

show ipv6 neighbors dynamic The command is used to view all dynamic neighbor table entries.

show ipv6 neighbors static The command is used to view all static neighbor table entries.

【example】

#View all neighbor table entries.

Switch#configure terminal

Switch(config)#show ipv6 neighbors all

Information of neighbors

IpAddress Mac_Address Vlan Port Type Status ExpireTime 2000::1
00:00:11:01:01:01 1 0/0/1 static PERMANENT --

fe80::288:88ff:fe30:4011 00:88:88:30:40:11 1 0/0/33 dynamic REACHABLE 27 sec

fe80::2e0:4cff:fe88:99c1 00:e0:4c:88:99:c1 1 0/0/33 dynamic REACHABLE 27 sec

fe80::2e0:61ff:fe09:1969 00:e0:61:09:19:69 1 0/0/33 dynamic STALE --

fe80::2e0:61ff:fe09:199a 00:e0:61:09:19:9a 1 0/0/33 dynamic REACHABLE 25 sec

fe80::2e0:61ff:fe09:19b1 00:e0:61:09:19:b1 1 0/0/33 dynamic REACHABLE 27 sec

fe80::2e0:61ff:fe56:9add 00:e0:61:56:9a:dd 1 0/0/33 dynamic REACHABLE 27 sec

fe80::7edd:76ff:fe02:81a4 7c:dd:76:02:81:a4 1 0/0/33 dynamic REACHABLE 25 sec

fe80::7edd:76ff:fe02:8859 7c:dd:76:02:88:59 1 0/0/33 dynamic REACHABLE 25 sec

fe80::cc8a:d629:8fb9:130b 94:05:b6:5c:d8:1e 1 0/0/33 dynamic REACHABLE 17 sec

Total entries: 10, Printed entries: 10

show ipv6 neighbors display fields description information

Fields	Description
IpAddress	IP address
Mac_Address	MAC address
Vlan	VLAN ID

Port	Port ID
Type	Type:dynamic、static
Status	status
ExpireTime	Remaining aging time
Total entries	Total number of table entries
Printed entries	Number of displays

22.2.3 show ipv6 neighbors max-learning-num

【command】

show ipv6 neighbors max-learning-num

【config-mode】

Any configuration mode

【parameter】

None

【description】

show ipv6 neighbors max-learning-num The Command is used to view neighbor learning limit.

【example】

#Check the limit on the number of neighbors learning.

Switch#configure terminal

Switch(config)#show ipv6 neighbors max-learning-num

Max number of neighbors entries to learn: 2048

22.2.4 show ipv6 nd reachable-time

【command】

show ipv6 nd reachable-time

【config-mode】

Any configuration mode

【parameter】

None

【description】

show ipv6 nd reachable-time The command is used to view the configuration information of the reachable state time.

【example】

#View reachable status time configuration information.

Switch#configure terminal

Switch(config)#show ipv6 nd reachable-time

Neighbor reachable time of interface:

Interface name : VLAN-IF1

Time(s) : 30

Interface name : loopback0

Time(s) : 30

Interface name : superVLAN-IF1

Time(s) : 30

Total entries: 3 interface.

show ipv6 nd reachable-time display fields description

Fields	Description
Interface name	Interface name
Time(s)	Reachable state time
Total entries	Total number of table entries

22.2.5 show ipv6 nd ns retrans-time

【command】

show ipv6 nd ns retrans-time

【config-mode】

Any configuration mode

【parameter】

None

【description】

show ipv6 nd ns retrans-time The command is used to view the configuration information of the time period for sending NS messages.

【example】

#View the configuration information of the time period for sending NS messages.

Switch#configure terminal

Switch(config)#show ipv6 nd ns retrans-time

Neighbor retrans time of interface:

Interface name : VLAN-IF1

Time(s) : 1

Interface name : loopback0

Time(s) : 1

Interface name : superVLAN-IF1

Time(s) : 1800

Total entries: 3 interface.

show ipv6 nd ns retrans-time display fields description

Fields	Description
Interface name	Interface name
Time(s)	cycle time
Total entries	Total number of table entries

Chapter 23 DHCP server

23.1 DHCP Server Configuration Commands

23.1.1 dhcp-server

【command】

dhcp-server *server-id ip-address*

no dhcp-server *server-id*

【config-mode】

Global configuration mode

【parameter】

server-id:Server number,integer form,The value range is 1-256.

ip-address:ip address,dottedted decimal format,such as 192.168.1.1.

【description】

dhcp-server *server-id ip-address* The command is used to configure dhcp server.

no dhcp-server *group-value* The command is used to delete DHCP server configuration.

By default, there is no dhcp server present.

【example】

#Configure a dhcp server with ID 1 and IP address 192.168.1.26.

Switch#configure terminal

Switch(config)#dhcp-server 1 192.168.1.26

23.1.2 dhcp-server server-id

【command】

dhcp-server *server-id*

no dhcp-server *server-id*

【config-mode】

VLAN interface configuration mode

【parameter】

server-id:Server number,decimal integer format,The value range is 1-256.

【description】

dhcp-server *server-id* The command is used to enable dhcp server functionality.

no dhcp-server *server-id* The command is used to disable dhcp server functionality.

The device can successfully assign IP addresses as a server and must enable DHCP relay function. When the device receives a message from the client, it will use one of the following modes to process the message according to the configuration:

Server mode: When the configured dhcp server IP address is the IP address of the device, it indicates that the built-in DHCP server function is enabled. When a message is received from the DHCP client, addresses of the same address segment will be allocated from the local DHCP server's address pool based on the "giaddr" fields in the message.

Relay mode: When the configured dhcp server IP is not the IP address of this device, it indicates the use of an external DHCP server. When receiving a message from a DHCP client, the message is forwarded to an external DHCP server, which assigns an address.

【example】

#Enabling dhcp server functionality on a regular VLAN interface.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#dhcp-server 1

23.1.3 dhcp-server ip-pool

【command】

dhcp-server ip-pool *pool-name*

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

【config-mode】

Global configuration mode

【parameter】

pool-name:address pool name,string format,The value range is 1-32 characters.

【description】

dhcp-server ip-pool *pool-name* The command is used to create an address pool and enter address pool configuration mode

no dhcp-server ip-pool *pool-name* The command is used to delete the configuration of the address pool

【example】

#Create an ip pool named pool

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

23.1.4 gateway

【command】

gateway *ip-address mask*

【config-mode】

Address pool configuration mode

【parameter】

ip-address:ip address,dottedted decimal format,such as 192.168.1.1.

mask:subnet mask,dotted decimal format,such as 255.255.255.0.

【description】

gateway *ip-address mask* The command is used to configure the gateway corresponding to the address in the pool.

If 'router' is configured, the DHCP client uses the router address as the gateway, otherwise the address configured in 'gateway' is used as the gateway address of the DHCP client.

【example】

#Configure the gateway address of the DHCP client to 192.168.1.28.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#gateway 192.168.1.28 255.255.255.0

23.1.5 section

【command】

section *section-id start-ip end-ip*

no section *section-id*

【config-mode】

Address pool configuration mode

【parameter】

section-value:address segment number,decimal integer format,the value range is 0-7.

start-ip:ip address,dottedted decimal format,such as 192.168.1.1.

end-ip:ip address,dottedted decimal format,such as 192.168.1.10.

【description】

section *section-id start-ip end-ip* The command is used to configure assignable address segments.

no section *section-id* The command is used to delete assignable address segments.

Each address segment can be configured with a maximum of 1024 IP addresses, and a total of 8 address segments can be configured in the same address pool. The IP address must remain in the same network segment as the gateway address.

【example】

#Configure the assignable address range in the DHCP address pool to 192.168.1.1-192.168.1.20.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#section 0 192.168.1.1 192.168.1.20

23.1.6 lease

【command】

lease *ddd:hh:mm*

no lease

【config-mode】

Address pool configuration mode

【parameter】

ddd:days,the maximum value cannot exceed 999 days,value range is 0-999.

hh:hours,the value range is 0-23.

mm:minutes,the value range is 0-59.

【description】

lease *ddd:hh:mm* The command is used to configure the lease time of the IP address.

no lease The command is used to restore the lease time to the default value.

By default, the lease term is 12 hours.

【example】

#Configure the address lease duration assigned to DHCP clients to be 10 minutes.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#lease 000:00:10

23.1.7 dns-list

【command】

dns-list { **primary-ip** | **second-ip** | **third-ip** | **fourth-ip** } *ip-address*

no dns-list { **primary-ip** | **second-ip** | **third-ip** | **fourth-ip** }

【config-mode】

Address pool configuration mode

【parameter】

ip-address:ip address,dottedted decimal format,such as 192.168.1.1.

【description】

dns-list { primary-ip | second-ip | third-ip | fourth-ip } *ip-address* The command is used to configure DNS servers.

no dns-list { primary-ip | second-ip | third-ip | fourth-ip } The command is used to delete DNS servers.

Each address pool can be configured with up to 4 DNS server addresses. The DHCP server assigns IP addresses to clients and also sends domain names to them. By default, no DNS server is configured.

【example】

#Configure the DNS server address to 8.8.8.8.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#dns-list primary-ip 8.8.8.8

23.1.8 domain-name

【command】

domain-name *name-value*

no domain-name

【config-mode】

Address pool configuration mode

【parameter】

name-value:domain name,string format,value range: 1-32 characters.

【description】

domain-name The command is used to configure domain name.

no domain-name The command is used to delete domain name.

【example】

#Configure the domain name of the DHCP server to test.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#domain-name test

23.1.9 nbns-list

【command】

nbns-list { primary-ip | second-ip }

no nbns-list { primary-ip | second-ip }

【config-mode】

Address pool configuration mode

【parameter】

None

【description】

nbns-list { primary-ip | second-ip } *ip-address* The command is used to configure WINS server address.

no nbns-list { primary-ip | second-ip } The command is used to delete WINS server address.

【example】

#Configure the wins server address assigned to DHCP clients.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#nbns-list primary-ip 192.168.2.1

Switch(config-ip-pool-pool)#nbns-list second-ip 192.168.4.10

23.1.10 forbidden-ip

【command】

forbidden *ip-address*

no forbidden *ip-address*

【config-mode】

Address pool configuration mode

【parameter】

ip-address:ip address,dotted decimal format,such as 192.168.1.1.

【description】

forbidden *ip-address* The command is used to configure IP addresses that are prohibited from being assigned to clients.

no forbidden *ip-address* The command to delete previous configuration.

When the DHCP server allocates addresses, it is necessary to exclude IP addresses that have already been occupied, such as gateways, FTP servers, etc.

【example】

#Prohibit assigning IP addresses of 192.168.1.88 to clients.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#forbidden-ip 192.168.1.88

23.1.11 router

【command】

router *ip-address*

no router

【config-mode】

Address pool configuration mode

【parameter】

ip-address:ip address,dotted decimal format,such as 192.168.1.1.

【description】

router *ip-address* The command is used to configure the gateway address assigned to the client.

no router The command is used to delete the configured gateway address.

【example】

#Configure the gateway address assigned to the client as 192.168.2.1.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#router 192.168.2.1

23.1.12 option

【command】

option *option-value* **{ ascii** *ascii-value* **| hex** *hex-value* **| ip** *ip-address* **| sub-option** *sub-option-value* **}**

no option code [sub-option *sub-option-value* **]**

【config-mode】

Address pool configuration mode

【parameter】

option-value:dhcp custom options,decimal integer format,value range:4-254.

ascii-value:ASCII code value, string format, value range: 1-128 characters.

hex-value:hex value,hexadecimal format,value range:0-FF.

ip-address:ip address,dottedted decimal format,such as 192.168.1.1.

sub-option-value:DHCP sub option, decimal integer format, value range: 1-254

【description】

option *code* **{ ascii** *string* **| hex** *hex-value* **| ip** *ip-address* **| sub-option** *sub-option-code* **}** The command is used to configure

dhcp options.

no option code [sub-option *sub-option-code* **]** The command is used to delete dhcp options..

【example】

#Configure dhcp options option43,option56,option88,option89.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool x

Switch(config-ip-pool-x)#option 43 ascii 96100

Switch(config-ip-pool-x)#option 56 hex ab

Switch(config-ip-pool-x)#option 88 ip 192.168.1.66

Switch(config-ip-pool-x)#option 89 sub-option 66 ascii bb

23.1.13 dhcp-client bind

【command】

dhcp-client bind

no dhcp-client bind

【config-mode】

Global configuration mode

【parameter】

None

【description】

dhcp-client bind The command is used to enable the allocation of IP addresses to static bound table entries.

no dhcp-client bind The command is used to disable the allocation of IP addresses to static bound table entries.

【example】

#Enable the function of assigning IP addresses to static binding table entries.

Switch#configure terminal

Switch(config)#dhcp-client bind

23.1.14 dhcp-client bind ip-address mac-address vlan-id

【command】

dhcp-client bind [*ip-address mac-address vlan-id* **]**

no dhcp-client bind { all | *mac-address* **}**

【config-mode】

Global configuration mode

【parameter】

ip-address:ip address,dottedted decimal format,such as 192.168.1.1.

mac-address:mac address,hexadecimal format,such as 00:00:11:22:33:44.

vlan-id:vlan id,decimal integer format,value range: 1-4094.

【description】

dhcp-client bind *ip-address mac-address vlan-id* The command is used to configure static binding table entries.

no dhcp-client bind { all | *mac-address* **}** The command is used to delete static binding table entries.

【example】

#Configure static binding table entries to assign the specified IP address 192.168.1.56 to users with MAC address 00:00:00:11:11:11.

Switch#configure terminal

Switch(config)#dhcp-client bind 192.168.1.56 00:00:00:11:11:11 1

23.1.15 dhcp-client unbind-assign

【command】

dhcp-client unbind-assign

no dhcp-client unbind-assign

【config-mode】

Global configuration mode

【parameter】

None

【description】

dhcp-client unbind-assign The command is used to enable the allocation of IP addresses to unbound users.

no dhcp-client unbind-assign The command to cancel the function of assigning IPaddresses to unbound users.

【example】

#Enable IP allocation to unbound users in global mode.

Switch#configure terminal

Switch(config)#dhcp-client unbind-assign

23.1.16 unbind-client

【command】

unbind-client section *section-id*

no unbind-client section

【config-mode】

Address pool configuration mode

【parameter】

section-value:address segment number,decimal integer format,the value range is 0-7.

【description】

unbind-client section *section-id* The command is used to configure address segments that prioritize assigning IP addresses to users who do not match binding table entries.

no unbind-client section The command is used to cancel the address segment used for users who do not match bound table entries.

【example】

#Prioritize assigning IP addresses in address segment 0 to users who do not match binding table entries.

Switch#configure terminal

Switch(config)#dhcp-server ip-pool pool

Switch(config-ip-pool-pool)#unbind-client section 0

23.2 DHCP Server Monitoring and Debug Commands

23.2.1 show dhcp-server

【command】

show dhcp-server [*server-id* **]**

【config-mode】

Any configuration mode

【parameter】

server-id:server number,decimal integer format,the value range is 1-256.

【description】

show dhcp-server [*server-id* **]** The command is used to view the configuration of the dhcp server.

【example】

#View relevant information about dhcp server.

Switch#configure terminal

Switch(config)#show dhcp-server

Information global of dhcp server

DHCP server group : 1

IP adrress : 192.168.1.26

DHCP server group : 2

IP adrress : 192.168.2.26

Total entries:2

show dhcp-server display fields description

Fields	Description
DHCP server group	Server id
IP adrress	Server IP
Total entries	Total number of table entries

23.2.2 show dhcp-server clients

【command】

show dhcp-server clients [*ip-address* | *mac-address* | *pool-name* **]**

【config-mode】

Any configuration mode

【parameter】

ip-address:ip address,dottedted decimal format,such as 192.168.1.1.

mask:subnet mask, hexadecimal format, such as 255.255.255.0.

pool-value:address pool name,string format,the value range is 1-32 characters.

【description】

show dhcp-server clients [*ip-address* | *mac-address* | *pool-name* **]** The command is used to view server IP address allocation information.

【example】

#View server IP address allocation information.

Switch#configure terminal

Switch(config)#show dhcp-server clients

User MAC	Port	VID	IP	Bind Flag	Hostname
00:00:02:01:01:0a	e0/0/1	1	192.168.1.107	unbound	XINERTEL
00:00:02:01:01:0b	e0/0/1	1	192.168.1.108	unbound	XINERTEL
00:00:02:01:01:08	e0/0/1	1	192.168.1.105	unbound	XINERTEL
00:00:02:01:01:09	e0/0/1	1	192.168.1.106	unbound	XINERTEL
00:00:02:01:01:0c	e0/0/1	1	192.168.1.109	unbound	XINERTEL
00:00:02:01:01:03	e0/0/1	1	192.168.1.100	unbound	XINERTEL
00:00:02:01:01:06	e0/0/1	1	192.168.1.103	unbound	XINERTEL
00:00:02:01:01:07	e0/0/1	1	192.168.1.104	unbound	XINERTEL
00:00:02:01:01:04	e0/0/1	1	192.168.1.101	unbound	XINERTEL
00:00:02:01:01:05	e0/0/1	1	192.168.1.102	unbound	XINERTEL

Total entries: 10.

Show dhcp server clients display fields description

Fields	Description
User MAC	User Mac Address
Port	Port number
VID	VLAN ID
IP	IP address
Bind Flag	Is it a static binding address

Hostname	User Name
Total entries	Total number of table entries

23.2.3 show dhcp-server interface

【command】

show dhcp-server interface [vlan-interface *vlan-id* **| supervlan-interface** *supervlan-id* **]**

【config-mode】

Any configuration mode

【parameter】

vlan-id:vlan id,decimal integer format,value range: 1-4094.

supervlan-id:supervlan id,decimal integer format,value range: 1-128.

【description】

show dhcp-server interface [vlan-interface *vlan-id* **| supervlan-interface** *supervlan-id* **]** The command is used to view the dhcp server configuration referenced under the vlan interface.

【example】

#View the dhcp server configuration referenced under the vlan interface.

Switch#configure terminal

Switch(config)#show dhcp-server interface

Information interface of dhcp server

Interface name : VLAN-IF1

DHCP server group : 1,

Interface name : VLAN-IF2

DHCP server group : 2,

Total entries:2

show dhcp-server interface display fields description

Fields	Description
Interface name	Interface id
DHCP server group	Dhcp server number
Total entries	Total number of table entries

23.2.4 show dhcp-server ip-pool

【command】

show dhcp-server ip-pool { *pool-name* **[** *section-id***] | brief** }

【config-mode】

Any configuration mode

【parameter】

pool-value:address pool name,string format,the value range is 1-32 characters.

section-value:address segment number,decimal integer format,the value range is 0-7.

【description】

show dhcp-server ip-pool [*pool-name*] The command is used to view the configuration in the address pool.

show dhcp-server ip-pool *pool-name section-id* The command is used to view information in address segments.

show dhcp-server ip-pool brief The command is used to view brief information about address pools.

【example】

#View information about address pools.

Switch#configure terminal

Switch(config)#show dhcp-server ip-pool pool

Information of dhcp-server ip-pool

Ip-Pool name : pool

GateWay : 192.168.1.26

Subnet Mask : 255.255.255.0

Route Ip : 192.168.1.26

Lease Time : 1 days 00:00:00

Primary DNS : 8.8.8.8

Second DNS : 2.2.2.2

Third DNS : 0.0.0.0

Fourth DNS : 0.0.0.0

Primary wins : 192.168.2.1

Second wins : 192.168.4.1

Domain Name : test

Unbind-client section: 0

Customized option:

code	subcode	format	length	value
43	N/A	ASCII	5	96100
56	N/A	HEX	1	ab
66	66	IP	4	192.168.1.2
88	N/A	IP	4	192.168.1.66
89	66	ASCII	2	bb

SectionNo	StartIp	EndIp	Total	Used/Idle
0	192.168.1.100	192.168.1.200	101	10/91
1	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A

Total entries: 1

show dhcp-server ip-pool display fields description

Fields	Description
Ip-Pool name	Address pool name
GateWay	Gateway IP
Subnet Mask	Subnet mask of gateway address
Route Ip	Router ip
Lease Time	Lease time
Primary DNS	Primary DNS server
Second DNS	Second DNS server

Third DNS	Third DNS server
Fourth DNS	Fourth DNS server
Primary wins	Primary wins server
Second wins	Second wins server
Domain Name	Domain Name
Unbind-client section	Address segment assigned to users who do not match bound table entries
Customized option	Custom option
SectionNo	Address segment number
StartIp	Address segment start IP
EndIp	Address segment end IP
Total	Total number of address segments
Used/Idle	Address segment used/idle
Total entries	Total number of table entries

23.2.5 show dhcp-client bind

【command】

show dhcp-client bind [*ip-address* | *mac-address* **]**

【config-mode】

Any configuration mode

【parameter】

ip-address:ip address,dotted decimal format,such as 192.168.1.1.

mac-address:mac address,hexadecimal format,such as 00:00:11:22:33:44.

【description】

show dhcp-client bind [*ip-address* | *mac-address*] The command is used to view bound table entries.

【example】

#View configured binding table entries.

Switch#configure terminal

Switch(config)#show dhcp-client bind

Information of dhcp client bind

dhcp client bind: enable

dhcp client unbind assign: enable

Ip_Address Mac_Address Vlan

192.168.1.56 00:00:00:11:11:11 1

192.168.2.1 00:00:11:00:11:00 1

Total entries: 2.

show dhcp-client bind display fields description

Fields	Description
dhcp client bind	Binding-State:enble、disable

dhcp client unbind assign	Unbound user assigned address status:enable、disable
Ip_Address	Bind the user's IP address
Mac_Address	Bind the user's MAC address
Vlan	Bind the user's VLAN ID
Total entries	Total number of table entries

23.2.6 debug dhcp

【command】

debug dhcp

no debug dhcp

【config-mode】

Global configuration mode

【parameter】

None

【description】

debug dhcp The command is used to open dhcp debugging information.

no debug dhcp The command is used to turn off dhcp debugging information.

By default, the dhcp debugging function is turned off.

【example】

#Enable dhcp debugging information.

switch#configure terminal

switch(config)#debug dhcp

Chapter 24 DHCP relay

24.1 DHCP Relay Configuration Commands

24.1.1 dhcp-relay

【command】

dhcp-relay

no dhcp-relay

【config-mode】

Global/Port configuration mode

【parameter】

None

【description】

dhcp-relay The command is used to enable dhcp delay function.

no dhcp-relay The command is used to disable the dhcp delay function.

By default, the global dhcp delay function is in the disabled state, and the dhcp delay function under the port is in the enabled state.

【example】

#Enable dhcp delay function globally.

Switch#configure terminal

Switch(config)#dhcp-relay

24.1.2 dhcp-relay hide server-ip

【command】

dhcp-relay hide server-ip

no dhcp-relay hide server-ip

【config-mode】

Global configuration mode

【parameter】

None

【description】

dhcp-relay hide server-ip The command is used to enable the function of hiding server IP addresses.

no dhcp-relay hide server-ip The command is used to disable the function of hiding server IP addresses.

If the user does not want the DHCP client to know the address of the DHCP server, they can configure it to hide the real DHCP server address on the device that enables DHCP relay. If the device that enables DHCP relay happens to be the DHCP server, this feature is no longer applicable.

【example】

#Enable hidden server IP address function.

Switch#configure terminal

Switch(config)#dhcp-relay hide server-ip

24.1.3 dhcp-relay max-hops

【command】

dhcp-relay max-hops *hop-value*

no dhcp-relay max-hops

【config-mode】

Global configuration mode

【parameter】

*hop-value:*Maximum jump value, value range from 1 to 16.

【description】

dhcp-relay max-hops *hop-value* The command is used to configure the maximum number of hops for DHCP packet propagation.

no dhcp-relay max-hops The command is used to restore hops to the default value.

By default, the maximum number of hops for DHCP packet propagation is 8.

【example】

#Limit the maximum number of hops for DHCP packet propagation to 16.

Switch#configure terminal

Switch(config)#dhcp-relay max-hops 16

24.2 DHCP Relay Monitoring and Debug Commands

24.2.1 show dhcp-relay

【command】

show dhcp-relay

【config-mode】

Any configuration mode

【parameter】

None

【description】

show dhcp-relay The command is used to view the relevant configuration of dhcp delay.

【example】

#View the relevant configurations of dhcp relay.

Switch(config)#show dhcp-relay

Information of dhcp relay

DHCP relay status: enable

DHCP relay hide server ip: enable

DHCP relay max hops: 16

Information port of dhcp relay

Port DhcpRelay

e0/0/1 Enable

e0/0/2 Enable

e0/0/3 Enable

……

Total entries: 10.

show dhcp-relay display fields description

Fields	Description
DHCP relay status	The global state of dhcp relay:enable、disable
DHCP relay hide server ip	Hide the status of the server address function:enable、disable
DHCP relay max hops	Maximum number of hops allowed for dhcp message propagation
Information port of dhcp relay	Port Enable Status
Total entries	Total number of table entries

24.2.2 debug dhcp

【command】

debug dhcp

no debug dhcp

【config-mode】

Global configuration mode

【parameter】

None

【description】

debug dhcp The command is used to open DHCP debugging information.

no debug dhcp The command is used to turn off DHCP debugging information.

By default, the DHCP debug switch is turned off.

【example】

#Enable DHCP debugging information.

switch#configure terminal

switch(config)#debug dhcp

Chapter 25 DHCP option60

25.1 DHCP Option60 Configuration Commands

25.1.1 dhcp-option60 { equals | start-with } { ascii | hex }

【command】

dhcp-option60 { equals | start-with } { ascii | hex } *string-value* **gateway** *ip-address* **[dhcp-server** *server-id* **server-reply { ascii | hex }** *string-value* **]**

no dhcp-option60 { equals | start-with } { ascii | hex } *string-value*

【config-mode】

Vlan interface configuration mode

【parameter】

Equals: Indicates an exact match of content

Start with: indicates matching the starting content

Ascii: Indicates the ascii format

Hex: represents hexadecimal format

String value: The matching value, string format, with a maximum length of 50

Ip address: IP address, dotted decimal format, such as 192.168.1.10

Server id: Server ID,decimal integer format, ranging from 1 to 256

【description】

dhcp-option60 { equals | start-with } { ascii | hex }The command is used to configure the dhcp60 function.

no dhcp-option60 { equals | start-with } { ascii | hex }The command is used to delete the configuration of dhcp60.

By default, dhcp option60 is not configured.

【example】

#Configure dhch option60 under vlan interface 1.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#dhcp-option60 equals ascii test gateway 192.168.1.11

25.2 DHCP Option60 Monitoring and Debug Commands

25.2.1 show dhcp-option60

【command】

show dhcp-option60 [supervlan-interface *if-id* **| vlan-interface** *if-id* **]**

【config-mode】

Any configuration mode

【parameter】

if-id:Interface ID, decimal integer format, value range: Normal VLAN interface 1-4094, SuperVALNinterface 1-128.

【description】

show dhcp-option60 [supervlan-interface *if-id* **| vlan-interface** *if-id* **]** The command is used to view the relevant configuration information of dhcp option60.

【example】

#View the configuration information of dhcp option60.

Switch(config)#show dhcp-option60

VLAN-IF1

Config 1:

Ascii equals:test

Gateway: 192.168.1.11

Dhcp server:

Dhcp server reply:

show dhcp-option60 display fields description

Fields	Description

Ascii equals	Matching Content
Gateway	Gateway address
Dhcp server	Dhcp server ID
Dhcp server reply	The content responded by the dhcp server

Chapter 26 Routing Fundamentals

26.1 Routing foundation Configuring commands

26.1.1 router id

【command】

router id *router-id*

no router id

【config-mode】

Global configuration mode

【parameter】

router-id: The Router ID of the device , points are divided in a decimal format.

【description】

router-id The command is used for configure the static Router ID.

no router-id The command is used for delete the static Router ID.

By default , there is no static Router ID , using the dynamic Router ID.

The automatic acquisition principle of equipment Router ID is as follows:

First select the largest IP address of the Loopback interface as the Router ID.

If the Loopback interface does not configured , select the largest IP address of the other interface as Router ID .

【example】

#Configure the Router ID for the device to 1.1.1.1.

Switch#configure terminal

Switch(config)#router id 1.1.1.1

26.1.2 ip dlf cpu

【command】

ip dlf cpu

no ip dlf cpu

【config-mode】

Global configuration mode

【parameter】

none

【description】

ip dlf cpu The command is used for enables to send unknown packets to cpu.

no ip dlf cpu The command is used for disables to send unknown packets to cpu.

In default, enable to send unknown packets to cpu, namely configuration ip dlf cpu.

no ip dlf cpu Can cause no communication, please configure carefully.

【example】

#Enables cpu processing on unknown packets.

Switch#configure terminal

Switch(config)#ip dlf cpu

26.1.3 ip host-dlf cpu

【command】

ip host-dlf cpu

no ip host-dlf cpu

【config-mode】

Interface configuration mode

【parameter】

none

【description】

ip host-dlf cpu The command is used for enables to send unknown packets to cpu.

no ip host-dlf cpu The command is used for disables to send unknown packets to cpu.

In default, enable to send unknown packets to cpu, namely configuration ip host-dlf cpu。

no ip host-dlf cpu Can cause no communication, please configure carefully.

【example】

#Enable the cpu processing on the unknown message of the vlan 1 interface.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip host-dlf cpu

26.2 Routing foundation monitoring command

26.2.1 show router id

【command】

show router id

【config-mode】

Any configuration mode

【parameter】

none

【description】

show router id The command is used for view the configured Router ID.

【example】

#View the configured Router ID.

Switch#show router id

Current router id: 1.1.1.1

26.2.2 show ip route

【command】

show ip route [*ip-address* **[** *mask* **] | rib-stats]**

【config-mode】

Any configuration mode

【parameter】

ip-address: purpose ip,ip address format.

mask: Netmask, ip address format.

rib-stats: Route statistics.

【description】

show ip route The command is used for view the ipv4 global routing table

【example】

#View the IPV 4 global routing table information

Switch#show ip route

IP route information

DestIp/Mask	Proto	Distance	Metric	Nexthop	Interface
70.1.1.0/24	connected	0	1	*	VLAN-IF70
127.0.0.0/8	connected	0	1	*	LOOPBACK
127.0.0.0/24	kernel	0	0	*	LOOPBACK
192.0.0.0/8	connected	0	1	*	VLAN-IF1

Total entries: 4. Printed entries: 4.

show ip route field description

Field	Description

DestIp/Mask	Target network segment and mask length
Proto	Routing protocol
Distance	administrative distance
Metric	Overhead value
Nexthop	Route the next jump
Interface	Outgoing interface
Total entries	Total number of routes
Printed entries	Number of routes printed

26.2.3 show ip fdb

【command】

show ip fdb [*ip-address [mask]* **]**

【config-mode】

Global configuration mode

【parameter】

ip-address: The ip address, point split decimal format such as 192.168.1.1.

mask: Network mask, dot split decimal format, such as 255.255.0.0.

【description】

show ip fdb The command is used for view the network layer transfer publication information.

【example】

#View the network layer transfer publication information.

Switch(config)#show ip fdb

Information of L3 table

IP Address	MAC Address	VLAN	PORT	CreateTime	UpdateTime
192.168.1.111	N/A	N/A	N/A	00:16:40 1970/01/10	00:16:40 1970/01/10

Total entries: 1.

show ip fdb field description

Field	Description
IP Address	IP Address
MAC Address	MAC Address
VLAN	VLAN ID
PORT	port number
CreateTime	creation time
UpdateTime	refresh time
Total entries	Total number of table items

26.2.4 show ip lpm

【command】

show ip lpm

【config-mode】

Global configuration mode

【parameter】

none

【description】

show ip lpm The command is used for view the lpm information

【example】

#View the lpm information

Switch(config)#show ip lpm

Information of lpm table

IP Address	Net Mask	NextHop	MAC Address	PORT
192.168.1.0	255.255.255.0	192.168.1.150	N/A	N/A
192.168.255.0	255.255.255.0	192.168.255.1	N/A	N/A

Total entries: 2.

show ip lpm field description

Field	Description
IP Address	IP address
Net Mask	Network mask
NextHop	The next hop
MAC Address	MAC address
PORT	port number

Total entries	Total number of table items

26.2.5 show ip dlf cpu

【command】

show ip dlf cpu

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ip dlf cpu The command is used for view the status of the cpu on the unknown message.

【example】

#View the status of the cpu on the unknown message.

Switch#show ip dlf cpu

Ip dlf cpu : enable.

show ip dlf cpu field description

Field	Description
Ip dlf cpu	Enable state

26.2.6 show ip host-dlf cpu

【command】

show ip host-dlf cpu

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ip host-dlf cpu The command is used for view the status of the cpu on the unknown message.

【example】

#View the status of the cpu on the unknown message.

Switch#show ip host-dlf cpu

Interface : Host dlf cpu

VLAN-IF1 : Enabled

Total entries: 1 interface..

show ip host-dlf cpu Field Description

Field	Description
Interface	interface message
Host dlf cpu	Enable state

Chapter 27 IPv6 Routing foundation

27.1 IPv6 Routing base configuration command

27.1.1 ipv6 forwarding

【command】

ipv6 forwarding

no ipv6 forwarding

【config-mode】

Global configuration mode

【parameter】

none

【description】

ipv6 forwarding The command is used for turn on the IPv6 address forwarding function.

no ipv6 forwarding The command is used for turn off the IPV6 address forwarding function

By default, the IPV6 address forwarding function is off

【example】

#turn on the IPv6 address forwarding function.

Switch#configure terminal

Switch(config)#ipv6 forwarding

27.2 IPv6 routing foundation monitoring and debugging command

27.2.1 show ipv6 route

【command】

show ipv6 route

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ipv6 route The command is used for view the global routing table for IPv6.

【example】

#View the global routing table for IPv6.

Switch#show ipv6 route

IPv6 route information:

DestIp/len	Proto	Distance	Metric	Nexthop
::1/128	connected	0	1	*
2000::/64	ospf6	110	2	fe80::50
2000:0:0:1::/64	ospf6	110	101	fe80::50
2000:0:0:2::/64	ospf6	110	1001	fe80::50
3000::/64	static	1	0	5000::2
5000::/64	connected	0	1	*
6000::/64	connected	0	1	*
fe80::/64	connected	0	1	*
ff00::/8	kernel	0	256	*

Total entries: 9. Printed entries: 9.

show ipv6 route field description

field	description

DestIp/len	Target network segment and mask length
Proto	Routing protocol
Distance	Administrative distance
Metric	Cost
Nexthop	Next hop
Total entries	Total number of routes
Printed entries	Number of routes printed

27.2.2 show ipv6 fdb

【command】

show ipv6 fdb

【config-mode】

Global configuration mode

【parameter】

none

【description】

show ipv6 fdb The command is used for view the ipv6 network layer transfer publication information

【example】

#View the ipv6 network layer transfer publication information

Switch(config)#show ipv6 fdb

Information of L3 table

IP Address MAC Address VLAN PORT CreateTime UpdateTime

2000::1 N/A N/A N/A 06:42:52 1970/01/09 06:42:52 1970/01/09

Total entries: 1.

show ip fdb field description

Field	Description
IP Address	IP address
MAC Address	MAC address
VLAN	VLAN ID
PORT	Port number
CreateTime	creation time
UpdateTime	refresh time
Total entries	Total number of table items

27.2.3 show ipv6 lpm

【command】

show ipv6 lpm

【config-mode】

Global configuration mode

【parameter】

none

【description】

show ipv6 lpm The command is used for view the lpm information

【example】

#View the lpm information.

Switch(config)#show ipv6 lpm

Information of lpm table

IP Address NextHop MAC Address PORT

2000::/64 2000::1 N/A N/A

fe80::/64 fe80:: N/A N/A

Total entries: 2.

show ipv6 lpm field description

Field	Description
IP Address	IP address
NextHop	Next hop
MAC Address	MAC address
PORT	Port number
Total entries	Total number of table items

Chapter 28 Static routing

28.1 Static routing configuration command

28.1.1 ip route

【command】

ip route *ip-address mask next-hop* **[distance** *distance-value* **]**

no ip route { ***ip-address mask [next-hop* **] | static all }

【config-mode】

Global configuration mode

【parameter】

ip-address: destination network address.

mask: subnet mask.

next-hop: next hop address,must be the network where the device exists.

distance-value: manage distance values,integer form,the values range from 1-255

static all: represents all of the static routes.

【description】

ip route The command is used for configure static routes

no ip route The command is used for delete static routes

By default, the static routing is not configured.

【example】

#Configure a static route: 1.1.1.0/24,next hop address is: 50.1.1.2

Switch#configure terminal

Switch(config)#ip route 1.1.1.0 255.255.255.0 50.1.1.2

28.2 Static routing monitoring and debugging command

28.2.1 show ip route

【command】

show ip route [*ip-addresss [mask* **] | rib-stats]**

【config-mode】

Any configuration mode

【parameter】

ip-address: destination ip address

mask: subnet mask.

rib-stats: routing statistics for this information.

【description】

show ip route The command is used for view the IPV4 global routing table.

【example】

#view the IPV4 global routing table

Switch(config)#show ip route

IP route information

DestIp/Mask	Proto	Distance	Metric	Nexthop	Interface
1.1.1.0/24	static	1	0	50.1.1.2	VLAN-IF50
50.1.1.0/24	connected	0	1	*	VLAN-IF50
70.1.1.0/24	connected	0	1	*	VLAN-IF70
127.0.0.0/8	connected	0	1	*	LOOPBACK
127.0.0.0/24	kernel	0	0	*	LOOPBACK
192.0.0.0/8	connected	0	1	*	VLAN-IF1

Total entries: 6. Printed entries: 6.

show ip route field description

Field	Description
DestIp/Mask	Destination ip address and Mask length
Proto	Routing protocol
Distance	Administrative distance
Metric	Cost
Nexthop	Route next hop
Interface	Outgoing interface
Total entries	Total number of routes
Printed entries	Number of routes printed

Chapter 29 IPv6 Static routing

29.1 IPv6 Static routing configuration command

29.1.1 ipv6 route

【command】

ipv6 route *{ ipv6-address/length | ipv6-address mask } next-hop*

no ipv6 route *{ ipv6-address/length | ipv6-address mask } next-hop*

【config-mode】

Global configuration mode

【parameter】

ipv6-address/length: Purpose network address and mask length.

ipv6-address: Objective Network address

mask: Subnet mask

next-hop: Next hop address.

【description】

ipv6 route The command is used for configure the IPv6 static routing

no ipv6 route The command is used for remove the IPv6 static route.

By default, the IPv6 static routing is not configured.

【example】

#Configure an IPv6 static route: 2000::/32， the next hop address is: 5000::2。

Switch#configure terminal

Switch(config)#ipv6 route 2000::/32 5000::2

29.2 IPv6 Static routing monitoring and debugging command

29.2.1 show ipv6 route

【command】

show ipv6 route

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ipv6 route The command is used for view the global routing table for IPv6.

【example】

#View the global routing table information for IPv6

Switch(config)#show ipv6 route

IPv6 route information:

DestIp/len	Proto	Distance	Metric	Nexthop
::1/128	connected	0	1	*
2000::/32	static	1	0	5000::2
2000::/64	ospf6	110	2	fe80::50
2000:0:0:1::/64	ospf6	110	101	fe80::50
2000:0:0:2::/64	ospf6	110	1001	fe80::50
3000::/64	static	1	0	5000::2
5000::/64	connected	0	1	*
6000::/64	connected	0	1	*
fe80::/64	connected	0	1	*
ff00::/8	kernel	0	256	*

Total entries: 10. Printed entries: 10.

Table show ipv6 route field description

field	description
DestIp/len	Target network segment and mask length
Proto	Routing protocol
Distance	Administrative distance
Metric	Cost
Nexthop	Route the next hop
Total entries	Total number of routes
Printed entries	Number of routes printed

Chapter 30 RIP

30.1 RIP Configuring commands

30.1.1 router rip

【command】

router rip

no router rip

【config-mode】

Global configuration mode

【parameter】

none

【description】

router rip The command is used for Enable the RIP routing protocol, and go into the RIP configuration mode.

no router rip The command is used for Turn off the RIP routing protocol, and clear the RIP-related configuration.

By default, the RIP routing protocol is not enabled

【example】

#Enable the RIP routing protocol.

Switch#configure terminal

Switch#(config)#router rip

Switch#(config-router-rip)#exit

30.1.2 network

【command】

network *ip-address*

no network ip-address

【config-mode】

RIP configuration mode

【parameter】

ip-address: the interface ip address.

【description】

Network The command is used for start the RIP protocol for the specified network segment.

no network The command is used for close the RIP protocol for the specified network segment.

By default, no network segment starts the RIP protocol.

【example】

#start rip on 192.168.2.3 network address of the interface 1.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#network 192.168.2.3

30.1.3 ip rip authentication

【command】

ip rip authentication mode { md5 key-chain *key-chain-name* **| text passwd** *password* **}**

no ip rip authentication

【config-mode】

Interface configuration mode

【parameter】

mode md5: Authauthentication type, MD5 encryption authentication method.

mode text: Certification type, indicating the clear certification method.

key-chain *key-chain-name*: MD5 certified key name with a range of 1-32 characters.

passwd *password*: Clear text authentication password, the value range of 1-16 characters.

【description】

ip rip authentication The command is used for open the RIP authentication.

no ip rip authentication: The command is used for restore default situation.

By default, the interface does not enable the RIP authentication.

【example】

#Configure RIP authentication under VLAN 50 interface.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#ip rip authentication mode text passwd 123456

30.1.4 aggregate-address

【command】

aggregate-address *network/length*

no aggregate-address *network/length*

【config-mode】

RIP configuration mode

【parameter】

network/length: Network address / mask length, which represents the aggregated route.

【description】

aggregate-address The command is used for configure Aggregate Routing.

no aggregate-address The command is used for remove Aggregate Routing.

By default, no routing aggregation was performed.

After the aggregated route is configured, whether an aggregated route is generated depends on the existence of the detailed routes. If there is no detailed route that can be aggregated, the aggregated route will not be generated.

The tag of the aggregated route is 0, and the routing measure value is the minimum value in the detail routing. RIPv1 does not support aggregate routing by command.

【example】

#Configure routing aggregation, aggregated to 10.10.0.0/16.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#aggregate-address 10.10.0.0/16

30.1.5 default-information originate

【command】

default-information originate

no default-information originate

【config-mode】

RIP configuration mode

【parameter】

none

【description】

default-information originate The command is used for configuration introduces default routing and notifications.

no default-information originate The command is used for cancel the default routing notification.

By default, the default routing notification function is not configured.

After announcing the default routing, notify a 0.0.0.0/0 route as the default gateway, and avoid multiple RIP devices in the same RIP network to prevent a routing loop.

【example】

#Enable RIP to introduce the default routing functionality

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#default-information originate

30.1.6 default-metric

【command】

default-metric *metric-value*

no default-metric

【config-mode】

RIP configuration mode

【parameter】

metric-value: The default measure value for RIP republish routing, ranging from 1-16.

【description】

default-metric The command is used for configure the default measure value for the RIP republishing routes.

no default-metric The command is used for the default metric value for the recovery RIP republish route is the default value.

By default, the default RIP release route default measure is 1.

【example】

#Configure the RIP republish routing whose default measure value is 3

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#default-metric 3

30.1.7 distance

【command】

distance *distance-value*

no distance

【config-mode】

RIP configuration mode

【parameter】

distance-value: Administrative distance values of RIP routing, and the values range from 1-255.

【description】

distance The command is used for configure the managed distance values for the RIP routing.

no distance The command is used for the managed distance value for the restored RIP route is the default value.

The default value for the managed distance value for RIP routing is 120.

Route management distance is used to elect the best route between different routing protocols, and the smaller the value, the more preferred.

【example】

#Configure the RIP routing with a managed distance value of 100.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#distance 100

30.1.8 distribute-list

【command】

distribute-list { *acl* | **prefix** *prefix-name* } { **in** | **out** } [**supervlan-interface** *interface-id* | **vlan-interface** *interface-id*]

no distribute-list { *acl* | **prefix** *prefix-name* } { **in** | **out** } [**supervlan-interface** *interface-id* | **vlan-interface** *interface-id*]

【config-mode】

RIP configuration mode

【parameter】

acl: Access control list, support for id-based and name formats.

The id range of the IP standard access control list is 1-99,1300-1999.

The id range of the IP extended access control list is 100-199 and 2000-2699.

Acl name can have a string length of 1-32.

prefix-name: Prefix list name, input string length of 1-32.

in: Denotes those acting on the learned RIP route.

out: Represents the RIP route acting on the announcement out.

interface-id: The interface that the order takes effect.

【description】

distribute-list The command is used for configure the RIP routing and filtering function.

no distribute-list The command is used for cancel the RIP routing filtering function.

By default, the RIP routing filtering function is not configured.

After the RIP routing filtering function is enabled, only the routing that meets the conditions can be learned or notified.

This command can be configured to filter in both directions and specify filtered interfaces for all interfaces when not specified.

【example】

#Configure the filtering function in the routing direction of the ACL mode.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip access-list 1 deny 2.2.2.2 0.0.0.0

Switch(config-router-rip)#distribute-list 1 out

#Configure the filtering function on the routing orientation in the prefix list mode.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip prefix-list test permit 3.3.3.0/24

Switch(config-router-rip)#distribute-list prefix test in

30.1.9 offset-list

【command】

offset-list *acl-name* **{ in | out }** *metric-value* **[{supervlan-interface | vlan-interface}** *interface-id* **]**

no offset-list *acl-name* **{ in | out }** *metric-value* **[{supervlan-interface | vlan-interface}** *interface-id* **]**

【config-mode】

RIP configuration mode

【parameter】

acl-name: IP access control list name, for the 1-32 length string.

in: Indicates the modified learned route.

out: Represents the route out of the revised announcement.

metric-value: Set the incr metric value, take the value range 0-16.

interface-id: Interface number, and the value range is determined by the interface type.

【description】

offset-list The command is used to incr the specified route metric value.

no offset-list The command is used to delete configuration.

By default, no metric values for any RIP route.

Specifies the matching routing metric value in the modified access list, addresses the learned route on the incoming route and the outgoing route, and can be subdivided into the RIP interface.

【example】

#incr the route matching ACL 1 metric 10.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip access-list 1 permit 1.1.1.0 0.0.0.255

Switch(config-router-rip)#offset-list 1 in 10

30.1.10 redistribute

【command】

redistribute { bgp | connected | isis | ospf | static } [metric *metric-value* **] [route-map** *route-map-name* **]**

no redistribute { bgp | connected | isis | ospf | static }

【config-mode】

RIP configuration mode

【parameter】

bgp: Represents the BGP routing.

connected: Indicates direct routing.

isis: Represents an ISIS route.

ospf: Represents an OSPF routing.

static: Indicates static routing.

metric-value: Set the metric value, take the value range 0-16.

route-map-name: Applied route policy name, up to 32 characters.

【description】

Redistribute The command is used for configure the RIP routing redistributing function, and the routes being redistributed will be redistributed via the RIP routing.

no redistribute The command is used for cancel RIP route redistribute.

By default, RIP routing redistribute is not configured.

When redistributing, you can specify the metric value of the redistribution protocol and match the routing policy.

Notes:

l When RIP republishes the route, it references the route-map only when it publishes the route outward

【example】

#Configure RIP to republish the static route and set the measurement value to 3.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#redistribute static metric 3

30.1.11 route

【command】

route *network/length*

no route *network/length*

【config-mode】

RIP Configuration mode

【parameter】

network/length: Network address / mask length

【description】

route The command is used for configure a static RIP route

no route The command is used for remove the static RIP route.

By default, the static RIP routing is not configured.

【example】

#Configure a static RIP route: 1.1.1.0/24.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route 1.1.1.0/24

30.1.12 timers basic

【command】

timers basic *update-value timeout-value garbage-collection-value*

no timers basic

【config-mode】

RIP configuration mode

【parameter】

update-value: Routing update time, in seconds, the value range is: 5-65535, the default value is 30.

timeout-value: Route timeout time, in seconds, the value range is: 5-65535, the default value is 180.

garbage-collection-value: Garbage recovery time, per unit of seconds, the value range is: 5-65535, the default value is 120.

【description】

timers basic The command is used for configure the update time, timeout time, and garbage recycling time of the RIP routing.

no timers basic The command is used for restore the default value for the RIP timer

Update Time indicates how long the route is updated; timeout time indicates how long after the update message is received, the route will become invalid and the metric value becomes 16 hops; after the mevalue of the route becomes 16, the recycling timer will be enabled. If no update message is received in the counter, the route will be deleted.

【example】

#The configuration route has an update time of 40 seconds, a timeout time of 200 seconds, and a garbage recovery time of 150 seconds.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#timers basic 40 200 150

30.1.13 passive-interface

【command】

passive-interface { default | supervlan-interface *interface-id* **| vlan-interface** *interface-id* **}**

no passive-interface { default | supervlan-interface *interface-id* **| vlan-interface** *interface-id* **}**

【config-mode】

RIP configuration mode

【parameter】

default: Represents all of the interfaces.

interface-id: Interface id。

【description】

passive-interface The command is used for configure the RIP passive interface

no passive-interface The command is used for cancel the RIP passive interface

By default, there is no RIP passive interface.

The RIP passive interface can receive routing update messages and will not send routing update messages.

【example】

#Configure interface 1 as a passive interface.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#passive-interface vlan-interface 1

30.1.14 ip rip receive version

【command】

ip rip receive version { 1 | 2 [bcast | mcast] }

no ip rip receive version

【config-mode】

Interface configuration mode

【parameter】

1: The RIP only receives the RIPv1 messages.

2: The RIP only receives the RIPv2 messages.

2 bcast: RIP can receive RIPv1 and RIPv2 messages.

2 mcast: The RIP only receives the RIPv2 messages.

【description】

ip rip receive version The command is used for configure the RIP to process the version number of the received message on the interface

no ip rip receive version The command is used for cancel the version number of RIP processing received packets on the interface.

By default, the interface receives the version of 2 bcast, indicating receiving the RIPv1 and RIPv2 packets.

Notes:

The interface version number is preferred to the RIP global version number. After configthe interface version number, the global version number is configured with the version command. The RIP still uses the interface version number, and the global version number is used only used when the interface to send the version number is not configured.

【example】

#The received version of the configured VLAN 50 interface is RIPv 2.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#ip rip receive version 2

30.1.15 ip rip send version

【command】

ip rip send version { 1 | 2 [bcast | mcast] }

no ip rip send version

【config-mode】

Interface configuration mode

【parameter】

1: The RIP only sends the RIPv1 messages.

2: RIP only sends RIPv2 messages.

2 bcast: The RIP sends both RIPv1 and RIPv2 messages.

2 mcast: The RIP only sends the RIPv2 messages.

【description】

ip rip send version The command is used for configure the RIP to process the version number of the sending message on the interface.

no ip rip send version The command is used for cancel the version number of RIP on the interface.

By default, the interface sends the RIP version to 2.

Notes:

The interface version number is preferred to the RIP global version number. After configthe interface version number, the global version number is configured with the version command. The RIP still uses the interface version number, and the global version number is used only used when the interface to send the version number is not configured.

【example】

#Configure the VLAN 50 interface to send messages for both RIPv1 and RIPv2.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#ip rip send version 2 bcast

30.1.16 version

【command】

version { 1 | 2 }

no version

【config-mode】

RIP configuration mode

【parameter】

1: RIP version 1.

2: RIP version 2.

【description】

version The command is used for configure the RIP global version number to support RIPv1 and RIPv2.

no version The command is used for restore the default RIP default version number.

By default, the version number is RIPv2 and the version number 2 bcast, indicating RIPv1 and RIPv2 messages.

Notes:

The interface version number is preferred to the RIP global version number. After configthe interface version number, the global version number is configured with the version command. The RIP still uses the interface version number, and the global version number is used only used when the interface to send the version number is not configured.

【example】

#Configure the RIP version to 2.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#version 2

30.1.17 ip rip split-horizon

【command】

ip rip split-horizon

no ip rip split-horizon

【config-mode】

Interface configuration mode

【parameter】

none

【description】

ip rip split-horizon The command is used for configure the interface to enable the horizontal segmentation function.

no ip rip split-horizon The command is used for cancel the horizontal segmentation function of the interface.

By default, the interface enables the horizontal segmentation function.

Horizontal segmentation is a strategy to avoid routing loops. After learning routing from an interface, the horizontal segmentation method will no longer announce this part of the route from the interface.

【example】

#Configure the RIP to turn off the horizontal segmentation function under the interface vlan 50.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#no ip rip split-horizon

30.1.18 ip rip split-horizon poisoned-reverse

【command】

ip rip split-horizon poisoned-reverse

no ip rip split-horizon poisoned-reverse

【config-mode】

Interface configuration mode

【parameter】

none

【description】

ip rip split-horizon poisoned-reverse The command is used for configure the interface to enable the toxicity reversal function.

no ip rip split-horizon poisoned-reverse The command is used for cancel the toxicity reversal function of the interface.

By default, the interface does not turn on the toxicity reversal function.

Toxicity reversal is a strategy to avoid the routing loop. After learning routing from an interface, the toxicity reversal mode will notify this partial route, but the number of routing jumps is 16.

【example】

#Configured to enable the toxicity reversal function under the interface vlan 50.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#ip rip split-horizon poisoned-reverse

30.1.19 key chain

【command】

key chain *key-chain-name*

no key chain *key-chain-name*

【config-mode】

RIP configuration mode

【parameter】

key-chain-name: The name of the key chain with a transformable string length of 1-32.

【description】

key chain The command is used for configure the name of the key chain, and go into the key chain configuration mode

no key chain The command is used for delete the configured key chain.

By default, the key chain is not configured.

【example】

#Configure the RIP keychain name to test and go into keychain configuration mode.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#key chain test

Switch(config-router-keychain)#

30.1.20 key

【command】

key *key-identifier-number*

no key *key-identifier-number*

【config-mode】

Keychain configuration mode

【parameter】

key-identifier-number: Key identification number, the value range is 0-255.

【description】

key The command is used for configure the key identification number, and enter into the keychain-key configuration mode.

no key The command is used for delete the configured key identity.

The default, the key identification number is not configured.

【example】

#Configure the key ID 1 in the key chain test.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#key chain test

Switch(config-router-keychain)#key 1

Switch(config-router-keychain-key)#

30.1.21 key-string

【command】

key-string *key-value*

no key-string

【config-mode】

keychain-key configuration mode

【parameter】

key-value: Authenticate password string, can input the string length of 1-16.

【description】

key-string The command is used for configure the RIP authentication password string.

no key-string The command is used for delete the configured authentication password string.

By default, the authentication password is not configured.

【example】

#Configure the RIP authentication password string to "test1234".

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#key chain test

Switch(config-router-keychain)#key 1

Switch(config-router-keychain-key)#key-string test1234

30.1.22 accept-lifetime

【command】

accept-lifetime *start-time start-day start-month start-year* { **duration** *duration-value* | **infinite** | *end-time end-day end-month end-year* }

【config-mode】

keychain-key configuration mode

【parameter】

start-time start-day start-month start-year: Password start effective time, time / minute / second / day / month / year.

end-time end-day end-month end-year: Password end effective time, time / minute / second / day / month / year.

Days range from 1-31, months to 1-12, and years to 1993-2035.

duration-value: Length of effective time sustained after start time, in seconds, ranged from 1-2147483646.

infinite: The password has been valid since the valid time.

【description】

accept-lifetime The command is used for configure the receive survival period of the RIP authentication key.

The receive password is always valid by default.

After receiving the survival authentication period, the authentication information is only verified during the survival time, that is, the routing information can be successfully learned during the time period, and the authentication will fail.

The validity of a Key ID is divided into sending and receiving in two directions. The The command is used for sets the effective time of receiving the password, and the command send-lifetime is used to set the effective time of sending the password.

Timing automatic switch password, in different time periods of using different passwords, greatly increase the security of the password.

Key ID Which valid time configuration is used depends on the time pattern of the belonging keychain.

The effective time is based on the system time (regardless of the difference in time zones), so the system time of the authentication parties must be consistent.

【example】

#The receiving survival period for the configured RIP authentication key is 2022 / 11 / 22 12:00:00-2022 / 12 / 22 16:00:00.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#key chain test

Switch(config-router-keychain)#key 1

Switch(config-router-keychain-key)# accept-lifetime 12:00:00 22 11 2022 16:00:00 22 12 2022

30.1.23 send-lifetime

【command】

send-lifetime *start-time start-day start-month start-year* { **duration** *duration-value* | **infinite** | *end-time end-day*

end-month end-year }

【config-mode】

keychain-key configuration mode

【parameter】

start-time start-day start-month start-year: start time, time / minute / second / day / month / year.

end-time end-day end-month end-year: End time, time / minute / second / day / month / year.

Days range from 1-31, months to 1-12, and years to 1993-2035.

duration-value: Duration of the key, with a value range of 1-2147483646.

infinite: the password has been valid since the valid time.

【description】

send-lifetime The command is used for configure the transmission lifetime of the RIP authentication key.

By default, the send password is always valid.

After the authentication survival period is sent, only the notification message can be learned through the authentication, but not during this period cannot be learned through the notification message.

【example】

#The transmission lifetime of the configured RIP authentication key is 2022 / 11 / 22 12:00:00-2022 / 12 / 22 16:00:00.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#key chain test

Switch(config-router-keychain)#key 1

Switch(config-router-keychain-key)#send-lifetime 12:00:00 22 11 2022 16:00:00 22 12 2022

30.1.24 route-map in

【command】

route-map *route-map-name* **in { supervlan-interface | vlan-interface }** *interface-id*

no route-map *route-map-name* **in { supervlan-interface | vlan-interface }** *interface-id*

【config-mode】

RIP configuration mode

【parameter】

route-map-name: route map name

in: It represents the entry direction, that is, the matching route graph when learning the route.

interface-id: Interface ID, the configuration range depends on the interface type.

【description】

route-map in The command is used for configure the routing map applied when the interface learns the routing.

no route-map in The command is used for restore the default situation.

By default, the route map is not applied.

Before applying a routing map, refer to the command : **route-map**。

【example】

#Configuration to apply routing maps when the vlan 50 interface learns routing.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#match metric 10

Switch(config-router-routemap-aa-1)#set metric 2

Switch(config-router-rip)#route-map aa in vlan-interface 50

30.1.25 route-map out

【command】

route-map *route-map-name* **out { supervlan-interface | vlan-interface }** *interface-id*

no route-map *route-map-name* **out { supervlan-interface | vlan-interface }** *interface-id*

【config-mode】

RIP configuration mode

【parameter】

route-map-name: route map name.

out: Indicate the direction, that is, matching the route graph when publishing the route.

interface-id: Interface ID, the configuration range depends on the interface type.

【description】

route-map out The command is used for configure the routing map applied when the interface publishes the routing.

no route-map out The command is used for restore the default situation.

By default, the route map is not applied.

Before you need to create the route map, refer to the command: **route-map**。

【example】

#Configure to apply the routing map when the vlan 50 interface publishes the routing.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#match metric 10

Switch(config-router-routemap-aa-1)#match metric 5

Switch(config-router-rip)#route-map aa out vlan-interface 50

30.2 RIP Monitoring and debugging commands

30.2.1 show rip route-table

【command】

show rip route-table

【config-mode】

Any configuration mode

【parameter】

none

【description】

show rip route-table The command is used for view the routing information for the RIP protocol.

【example】

#View the routing information for the RIP protocol.

Switch#show rip route-table

RIP route information

Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP

Sub-codes:

(n) - normal, (s) - static, (d) - default, (r) - redistribute,

(i) - interface

Network	Next Hop	Metric From	Tag Time(s)
R(s) 3.3.3.3/32	0.0.0.0	1 self	0
R(n) 5.0.0.0/24	50.1.1.2	1 50.1.1.2	0 158
R(n) 5.0.1.0/24	50.1.1.2	1 50.1.1.2	0 158
C(i) 50.1.1.0/24	0.0.0.0	1 self	0
C(i) 60.1.1.0/24	0.0.0.0	1 self	0

Total entries: 5.

show rip route-table Field Description

Field	Description
Codes	Indicates the routing protocol type: R - RIP: RIP protocol C - connected: Direct routing S - Static: static routing O - OSPF: OSPF routing B - BGP: BGP routing
Sub-codes	Represents the route introduction method: (n) - normal: The route learned (s) - static: configured static RIP routing (d) - default: Configured default route (r) - redistribute: Route distribute routes for other protocols (i) - interface: Interface route introduced through the network mode
Network	Target network segment
Next Hop	The next hop address of the route
Metric	The metric-value of the route
From	The source of routing
Tag	The tag value of the route
Time(s)	Route the remaining time of aging in seconds

30.2.2 show ip rip interface

【command】

show ip rip interface

【config-mode】

any configuration mode

【parameter】

none

【description】

show ip rip interface The command is used for view the interface information for the enable RIP protocol.

【example】

#View the interface information for the enable RIP protocol.

Switch#show ip rip interface

information of RIP status

---

interface= VLAN-IF50

auth = disable passwd = N/A state = active

Rx = 2 bcast Tx = 2 split = split

---

interface= VLAN-IF60

auth = disable passwd = N/A state = active

Rx = 2 bcast Tx = 2 split = split

show ip rip interface field description

Field	Description

interface	Interface that enables the RIP protocol.
auth	Description of whether the authentication is enabled: disable:Indicates that the authentication is not enabled. text: Represents the opening of the plaintext certification. md5: It the MD5 encryption authentication.
passwd	The authentication key, if it is clear, authentication is the password of authentication, if it is MD5 authentication, it is the name of key-chain.
state	Interface state, with active and passive two states, respectively active: Indicates that the rip is enabled and can receive and send updated messages passive: It means that rip is enabled and can only receive or send update messages
Rx	The RIP version number received by the interface, where: 1: Representing messages receiving only RIPv1 2: Receiving only RIPv2 messages 2 bcast: means receiving RIPv1 and RIPv2 messages
Tx	The RIP version number sent by the interface, where: 1: A message sending only RIPv1 2: A message that sends only RIPv2 2 bcast: a message sending both RIPv1 and RIPv2
split	There are three cases of split values, as follows: No: indicates off level segmentation and toxicity reversal;

Split: means to open the horizontal segmentation;

split & & poison: Open toxicity reversal;

30.2.3 show ip rip status

【command】

show ip rip status

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ip rip status The command is used for view the detailed run information for the enable RIP protocol.

【example】

#View the detailed run information for the enable RIP protocol.

Switch#show ip rip status

Routing Protocol is "rip"

Sending updates every 30 seconds with +/-50%, next due in 25 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Default redistribution metric is 1

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is 1, (prefix-list) aa

VLAN-IF50 incoming filtered by test

VLAN-IF60 outgoing filtered by test2

Redistributing: ospf

Default version control: send version 2, receive any version

Routing for Networks:

50.1.1.1

60.1.1.1

Routing Information Sources:

Gateway	BadPackets	BadRoutes	Distance	Last Update
50.1.1.2	0	0	120	00:00:05

Distance: (default is 120)

show ip rip status field description

Field	Description
Sending updates	Route update message transmission interval, which has a fluctuation range of 50%
next due	The remaining time when the next route update message is sent
Timeout	Route timeout time
garbage collect	After the garbage recovery time, the metric value of the route is 16 jump, and you need to wait for the garbage collect to timeout before deleting the route
Default redistribution metric	The default metric value for the republish route
Outgoing update filter list for all interface	Filtering rules for all outgoing interfaces (distribute-list)
Incoming update filter list for all interface	Filter rules for all incoming interfaces (distribute-list)
VLAN-IF50 outgoing filtered	Specify the Interface Exit Filtering Rule (distribute-list)

VLAN-IF60 incoming filtered	Specify the Interface Entry Filter Rule (distribute-list)
Redistributing	Routing protocol for republishing that supports republishing bgp, connect, isis, ospf, static
Default version control	Default to send and receive the RIP version
Routing for Networks	The interface address for enabling the RIP protocol
Routing Information Sources	Routing source information for the RIP
Gateway	Gateway, which indicates the next hop interface address of the route
BadPackets	Error message statistics
BadRoutes	Error-routing statistics
Distance	administrative distance
Last Update	When the updated message was recently received

30.2.4 debug rip

【command】

debug rip

no debug rip

【config-mode】

Global configuration mode

【parameter】

none

【description】

debug rip The command is used for turn on the RIP debugging master switch.

no debug rip The command is used for turn off the RIP debugging master switch.

By default, the RIP debugging master switch is turned off.

【example】

#Turn on the RIP debugging master switch.

Switch#configure terminal

Switch(config)#debug rip

30.2.5 debug ip rip

【command】

debug ip rip { events | packet [recv | send] | zebra }

no debug ip rip { events | packet [recv | send] | zebra }

【config-mode】

Global configuration mode

【parameter】

events: Event information debug switch.

packet: Message interaction information debugging switch.

recv: Receive the relevant information of the message.

send: Send the information related to the message.

zebra: Information debugging switch for zebra process interaction.

【description】

debug ip rip The command is used for open the relevant debugging information for the RIP.

no debug ip rip The command is used for turn off the relevant debugging information for the RIP.

By default, all of the RIP debug switches are turned off.

RIP debugging will take effect at the same time of **debug ip rip** and **debug rip**.

【example】

#Open the event debug information switch for the RIP.

Switch#configure terminal

Switch(config)#debug ip rip events

Switch(config)#debug rip

Chapter 31 RIPng

31.1 RIPng Configuring commands

31.1.1 router ripng

【command】

router ripng

no router ripng

【config-mode】

Global configuration mode

【parameter】

none

【description】

router ripng The command is used for open the RIPng protocol and enter the RIPng configuration mode.

no router ripng The command is used for remove the RIPng protocol and to remove the RIPng associated configuration.

By default, the RIPng protocol is not enabled.

【example】

#Configure to turn on the RIPng protocol and enter the RIPng configuration mode.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#

31.1.2 ipv6 router ripng

【command】

ipv6 router ripng

no ipv6 router ripng

【config-mode】

Interface configuration mode

【parameter】

None

【description】

ipv6 router ripng The command is used for Enable to interface with the RIPng function.

no ipv6 router ripng The command is used for Turn off the RIPng function of the interface.

By default, the interface does not enable the RIPng function.

【example】

#RIPng function enabling vlan 50 interface.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#ipv6 router ripng

31.1.3 aggregate-address

【command】

aggregate-address *network/length*

no aggregate-address *network/length*

【config-mode】

RIPng configuration mode

【parameter】

network/length: Network address / mask length, which represents the aggregated route.

【description】

aggregate-address The command is used for configure the aggregate routing.

no aggregate-address The command is used for remove aggregate routing.

By default, no routing aggregation was performed.

After an aggregated route is configured, no generating an aggregated route depends on the existence of detail routes, which does not occur if there is no aggregated route that can be aggregated.

【example】

#Configure an aggregate route: 2000:: / 16.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#aggregate-address 2000::/16

31.1.4 default-information originate

【command】

default-information originate

no default-information originate

【config-mode】

RIPng configuration mode

【parameter】

none

【description】

default-information originate The command is used for enable the RIPng notification default routing function.

no default-information originate The command is used for unnotify the default route function and remove the default route to the adjacent device.

In default, the default routing function is not enabled.

After announcing the default route, notify the route of: / 0 as the default gateway, avoiding multiple RIPng devices to prevent the routing loop.

【example】

#Enable the RIPng notification default routing function.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#default-information originate

31.1.5 default-metric

【command】

default-metric *metric-value*

no default-metric

【config-mode】

RIPng configuration mode

【parameter】

metric-value: Default measure, range from 1 to 16.

【description】

default-metric The command is used for configure the default metric value for the redistribution route.

no default-metric The command is used for restore the default metric value for the redistribution route.

By default, the RIPng redistribution route is 1.

【example】

#Configure the RIPng redistribution route with a metric value of 5.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#default-metric 5

31.1.6 distribute-list

【command】

distribute-list { *acl-name* | **prefix** *prefix-name* } { **in** | **out** } [**supervlan-interface** *interface-id* | **vlan-interface** *interface-id*]

no distribute-list { *acl-name* | **prefix** *prefix-name* } { **in** | **out** } [**supervlan-interface** *interface-id* | **vlan-interface** *interface-id*]

【config-mode】

RIPng configuration mode

【parameter】

acl-name: IPv6 access list name, take the value range of 1 to 32 characters.

prefix-name: IPv6 prefix list name from 1 to 32 characters.

in: Reacting the learned RIPng route.

out: Indicates the RIPng route acting on the notification out.

interface-id: With slogans, the configuration range depends on the interface type.

【description】

distribute-list The command is used for enable the RIPng routing filtering function, only the routes that meet the filtering conditions are added to the database or notified. This command can support access list, prefix list, can be configured to filter in two directions, and can specify the filtering interface.

no distribute-list The command is used for cancel the routing and filtering function.

Routing filtering is not enabled by default.

【example】

#Configure filtered routing against the ACL list acl-1, applied in the entry direction.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#ipv6 access-list acl-1 permit 2000::/64

Switch(config-router-ripng)#distribute-list acl-1 in

#Configuration filter routing according to the prefix list test, applied in the exit direction.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#ipv6 prefix-list test permit 3000::/64

Switch(config-router-ripng)#distribute-list prefix test out

31.1.7 ipv6 ripng split-horizon

【command】

ipv6 ripng split-horizon

no ipv6 ripng split-horizon

【config-mode】

Interface configuration mode

【parameter】

none

【description】

ipv6 ripng split-horizon The command is used for turn on the horizontal segmentation function.

no ipv6 ripng split-horizon The command is used for Turn off the horizontal segmentation function.

By default, the interface enables the horizontal segmentation function.

Horizontal segmentation is a strategy to avoid routing loops. After learning routing from an interface, the horizontal segmentation method will no longer announce this part of the route from the interface.

【example】

#Turn off the horizontal segmentation function of the interface vlan 50.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#no ipv6 ripng split-horizon

31.1.8 ipv6 ripng split-horizon poisoned-reverse

【command】

ipv6 ripng split-horizon poisoned-reverse

no ipv6 ripng split-horizon poisoned-reverse

【config-mode】

Interface configuration mode

【parameter】

none

【description】

ipv6 ripng split-horizon poisoned-reverse The command is used for turn on the toxicity reversal function.

no ipv6 ripng split-horizon poisoned-reverse The command is used for turn off the toxicity reversal function.

In default, turn off the toxicity reversal function.

Toxicity reversal is a strategy to avoid the routing loop. After learning the routing from an interface, the toxicity reversal mode will notify this partial route, but the number of routing jumps is 16.

【example】

#Open the toxicity reversal function of the interface vlan 50.

Switch#configure terminal

Switch(config)#interface vlan-interface 50

Switch(config-if-vlanInterface-50)#ipv6 ripng split-horizon poisoned-reverse

31.1.9 offset-list

【command】

offset-list *acl-name* { **in** | **out** } *metric-value* [**supervlan-interface** *interface-id* | **vlan-interface** *interface-id*]

no offset-list *acl-name* { **in** | **out** } *metric-value* [**supervlan-interface** *interface-id* | **vlan-interface** *interface-id*]

【config-mode】

RIPng configuration mode

【parameter】

acl-name: IPv6 access list name, up to 32 characters.

In: it means to modify the learned route.

Out: change the route of the announcement.

metric-value: increased measure value, ranging from 0 to 16.

interface-id: catch slogan, configuration range depends on the interface type.

【description】

offset-list The command is used for modify the specified RIPng routing metric value.

no offset-list The command is used for undo the modifications to the specified RIPng routing metric value.

By default, no metric values for any RIPng route.

Specify the matching routing metric value in the modified access list, for the learned route learned in the incoming route and the outgoing route, and subdivided into the RIPng interface.

【example】

#Set metric 10 for the learned route 4000:: / 64.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#ipv6 access-list aa permit 4000::/64

Switch(config-router-ripng)#offset-list aa in 10

31.1.10 redistribute

【command】

redistribute { bgp | connected | isis | ospf6 | static } [metric *metric-value* **] [route-map** *route-map-name*]

no redistribute { bgp | connected | isis | ospf6 | static }

【config-mode】

RIPng configuration mode

【parameter】

bgp: BGP routing.

connected: Direct routing

isis: ISIS routing

ospf6: OSPFv3 routing

static: static routing

metric-value: Measure value, ranging from 0 to 16.

route-map-name: Route map name, configuration range of 1 to 32 characters.

【description】

redistribute The command is used for enables RIPng to distribute other protocol routes.

no redistribute The command is used for undo the redistribution of the specified protocol routing.

In default, no other agreements were redistributed.

Notes:

When RIPng republishes routes, the route-map is only cited when the routes are released outward.

【example】

#Configure the RIPng redistribute OSPFV3 protocol.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#redistribute ospf6

31.1.11 timers basic

【command】

timers basic *update-value timeout-value garbage-collection-value*

no timers basic

【config-mode】

RIPng configuration mode

【parameter】

update-value: Routing update time in seconds, range from 5 to 65535. The default value is 30.

timeout-value: Route timeout time in seconds, range from 5 to 65535. The default value is 180.

garbage-collection-value: Garbage recovery time, unit in seconds, the value range is: 5~65535. The default value is 120.

【description】

timers basic The command is used for configure the update time, time out time, and garbage recovery time of RIPng route.

no timers basic The command is used for restore the default value for the RIPng timer.

update Time indicates how long the route is updated, timeout time indicates how long after the update message is received, the route will become invalid, the metric value becomes 16, and the metic value of the route becomes 16, the garbage recycling timer will be enabled. If no update message is received in the counter, the route will be deleted.

【example】

#The configuration route has an update time of 40 seconds, a timeout time of 200 seconds, and a garbage recovery time of 150 seconds.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#timers basic 40 200 150

31.1.12 route-map in

【command】

route-map *route-map-name* **in { supervlan-interface** *interface-id* **| vlan-interface** *interface-id* **}**

no route-map *route-map-name* **in { supervlan-interface** *interface-id* **| vlan-interface** *interface-id* **}**

【config-mode】

RIPng configuration mode

【parameter】

route-map-name: Route map name, configuration range of 1 to 32 characters.

in: Represents that the incoming direction is applying the route graph when learning the route.

interface-id: With slogans, the configuration range depends on the interface type.

【description】

route-map in The command is used for configuration in the incoming interface application routing map.

no route-map in The command is used for restore the default situation.

By default, the route map is not applied.

To create the route map before applying the route map, refer to the command: **route-map**.

【example】

#Create routing map aa, allow metric value of 10 routing through, and apply routing map at the incoming interface.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#match metric 10

Switch(config-router-routemap-aa-1)#exit

Switch(config-router-ripng)#route-map aa in vlan-interface 50

31.1.13 route-map out

【command】

route-map *route-map-name* **out** { **supervlan-interface** *interface-id* | **vlan-interface** *interface-id* }

no route-map *route-map-name* **out** { **supervlan-interface** *interface-id* | **vlan-interface** *interface-id* }

【config-mode】

RIPng configuration mode

【parameter】

route-map-name: Route map name, configuration range of 1 to 32 characters.

out: Show that the direction is that the route map is applied when the route is published.

interface-id: With the slogan, the configuration range depends on the interface type.

【description】

route-map out The command is used for apply a route map when configuring release routes.

no route-map in The command is used for restore the default situation.

By default, the route map is not applied.

To create the route map before applying the route map, refer to the command: route-map.

【example】

#Create a routing map aa: match the routing of metric 10 and apply the routing map in the direction of the interface.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#match metric 10

Switch(config-router-routemap-aa-1)#exit

Switch(config-router-ripng)#route-map aa out vlan-interface 50

31.2 The RIPng monitoring and debugging command

31.2.1 show ripng route-table

【command】

show ripng route-table

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ripng route-table The command is used for view the routing information for the RIPng protocol.

【example】

#View the routing information for the RIPng protocol.

Switch#show ripng route-table

RIPNG route information

Codes: R - RIPng, C - connected, S - Static, O - OSPF, B - BGP

Sub-codes:

(n) - normal, (s) - static, (d) - default, (r) - redistribute,

(i) - interface, (a/S) - aggregated/Suppressed

NetWork	Next Hop	Via	Metric	Tag	Time(s)
R(n) 2000::/64	fe80::50	VLAN-IF50	1	0	154
R(n) 3000::/64	fe80::60	VLAN-IF60	1	0	178
C(i) 5000::/64	::	self	1	0	
C(i) 6000::/64	::	self	1	0	

Total entries: 4. Printed entries: 4.

show ripng route-table field description

Field	Description
Codes	Indicates the routing protocol type: R - RIPng: the RIPng protocol C - connected: Direct connection route S - Static: a static route O - OSPF: OSPFV3 routing

	B - BGP: BGP routing
Sub-codes	Represents the route introduction method: (n) - normal: The learned route. (s) - static: configured static RIPng routing, configuration is not supported. (d) - default: Default routing for configuration. (r) - redistribute: Routing for redistributing other protocols. (I) - interface: the RIPng command via the interface. (A / S) - aggregated / Suppressed: aggregate routing and inhibitory routing.
Network	Target network segment
Next Hop	The next hop address of the route
Metric	The metric-value of the route
From	The source of routing
Tag	The tag value of the route
Time(s)	Route the remaining time of aging in seconds

31.2.2 show ipv6 ripng status

【command】

show ipv6 ripng status

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ipv6 ripng status The command is used for View the detailed run information of the enabling RIPng protocol.

【example】

#View the detailed run information of the enabling RIPng protocol.

Switch#show ipv6 ripng status

Routing Protocol is "ripng"

Sending updates every 30 seconds with +/-50%, next due in 4 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Default redistribution metric is 1

Outgoing update filter list for all interface is bb

Incoming update filter list for all interface is (prefix-list) aa

VLAN-IF50 outgoing filtered by bb

VLAN-IF60 incoming filtered by (prefix-list) bb

Redistributing: ospf6

Routing Information Sources:

Gateway	BadPackets	BadRoutes	Distance	Last Update
fe80::60	0	0	120	00:00:23
fe80::50	0	0	120	00:00:17

show ipv6 ripng status field description

Field	Description

Sending updates	Route update message transmission interval, which has a fluctuation range of 50%
next due	The remaining time when the next route update message is sent
Timeout	Route timeout time
garbage collect	After the garbage recovery time, the metric value of the route is 16 jump, and you need to wait for the garbage collect to timeout before deleting the route
Default redistribution metric	The default metric value for the republish route
Outgoing update filter list for all interface	Filtering rules for all outgoing interfaces (distribute-list)
Incoming update filter list for all interface	Filter rules for all incoming interfaces (distribute-list)
VLAN-IF50 outgoing filtered	Specify the Interface Exit Filtering Rule (distribute-list)
VLAN-IF60 incoming filtered	Specify the Interface Entry Filter Rule (distribute-list)
Redistributing	Routing protocol for republishing bgp, connect, isis, ospf 6, static
Routing Information Sources	Route source information for RIPng
Gateway	Gateway, which indicates the next hop interface address of the route
BadPackets	Error message statistics
BadRoutes	Error-routing statistics
Distance	administrative distance

Last Update	When the updated message was recently received

31.2.3 show ipv6 ripng interface

【command】

show ipv6 ripng interface

【config-mode】

Any configuration mode

【parameter】

none

【description】

show ipv6 ripng interface The command is used for view the interface information that enables the RIPng protocol.

【example】

#View the RIPng interface information

Switch#show ipv6 ripng interface

Information of RIPng status

---

interface= VLAN-IF50

state = active split = split && poison

---

interface= VLAN-IF60

state = active split = split

show ipv6 ripng interface field description

Field	Description
interface	vlan interface message
state	Interface state, with two active and passive states, respectively active: Open ripng, and can receive and send update messages passive: Open ripng, can only receive but can not send the update message
split	There are three cases of split values, as follows: No: indicates off level segmentation and toxicity reversal; Split: means to open the horizontal segmentation; split & & poison: Open toxicity reversal;

31.2.4 debug ripng

【command】

debug ripng

no debug ripng

【config-mode】

Global configuration mode

【parameter】

none

【description】

debug ripng The command is used for open the RIPng debug master switch.

no debug ripng The command is used for close the RIPng debug master switch.

By default, the RIPng debug master switch is turned off.

【example】

#Open the RIPng debug master switch.

Switch#configure terminal

Switch(config)#debug ripng

31.2.5 debug ipv6 ripng

【command】

debug ipv6 ripng { events | packet [recv | send] | zebra }

no debug ipv6 ripng { events | packet [recv | send] | zebra }

【config-mode】

Global configuration mode

【parameter】

events: Event information debug switch.

packet: Message interaction information debugging switch.

recv: Receive the relevant information of the message.

send: Send the information related to the message.

zebra: Information debugging switch for zebra process interaction.

【description】

debug ipv6 ripng The command is used for open the relevant debugging information for the RIPng.

no debug ipv6 ripng The command is used for close the relevant debugging information for the RIPng.

By default, all of the RIPng debug switches are turned off.

Need both **debug ipv6 ripng** and **debug ripng** for RIPng debugging will take effect.

【example】

#Open the event debug information switch for RIPng.

Switch#configure terminal

Switch(config)#debug ipv6 ripng events

Switch(config)#debug ripng

Chapter 32 OSPF

32.1 OSPF Configuring commands

32.1.1 router ospf

【command】

router ospf [*process-id*]

no router ospf [*process-id*]

【config-mode】

Global configuration mode

【parameter】

process-id: OSPF process number, and the values range from 1 to 10.

【description】

router ospf The command is used for turn on the OSPF protocol and enter the OSPF configuration mode.

no router ospf The command is used for remove the OSPF protocol and remove the OSPF related configuration.

The OSPF protocol is not enabled by default.

【example】

#Turn on the OSPF protocol and enter the OSPF configuration mode.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#

32.1.2 ospf router-id

【command】

ospf router-id *router-id*

no ospf router-id

【config-mode】

OSPF configuration mode

【parameter】

router-id: The Router ID of the equipment, points in decimal form.

【description】

ospf router-id The command is used for configure the Router ID of the OSPF.

no ospf router-id The command is used for restore the default situation.

By default, the device Router ID is automatically acquired.

Equipment Router ID automatic acquisition principles are as follows:

1. First, select the largest one from the IP address of the Loopback interface as the Router ID.

2. If no Loopback interface is configured, select the largest from the IP address of other interfaces as Router ID.

Devices running the OSPF protocol, there must be a Router ID for uniquely identifying a device within an OSPF autonomous system. The uniqueness of Router ID in the autonomous system needs to be guaranteed, otherwise it will affect neighbor building and routing learning.

【example】

#Configure OSPF Router id to 1.1.1.1.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#ospf router-id 1.1.1.1

32.1.3 network area

【command】

network *ip-address wildcard-mask* **area** *area-id*

no network *ip-address wildcard-mask* **area** *area-id*

【config-mode】

OSPF configuration mode

【parameter】

ip-address: The IP address, which must be a device interface IP.

wildcard-mask: Countermask, namely the reverse address mask, such as the mask 255.255.255.0 is 0.0.0.255. In the backmask, 0 is the placeholder, and 1 is the one that can be arbitrarily matched.

area-id:Area ID, there are two ways: one is the decimal number between 0 and 4294967295; the other is the IP address between 0.0.0.0 and 255.255.255.255.

【description】

network *ip-address wildcard-mask* **area** The command is used for enable the OSPF protocol and configure the home OSPF region.

no network *ip-address wildcard-mask* **area** The command is used for disable the OSPF protocol and configure the home OSPF region.

By default, the interface turns off the OSPF protocol.

The OSPF supports multiple processes, but one interface can only belong to one OSPF process and region.

【example】

#Open the VLAN 1 interface ospf protocol and specify the region as 0.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#network 192.168.1.10 0.0.0.255 area 0

32.1.4 area authentication

【command】

area *area-id* **authentication [message-digest]**

no area *area-id* **authentication**

【config-mode】

OSPF configuration mode

【parameter】

area-id: OSPF area ID, in two ways: one is decimal number between 0 and 42949967295; the other is IP address between

0.0.0.0 and 255.255.255.255.

Authentication:Indicates that the configuration authentication method is a simple text authentication.

authentication message-digest:Indicthat the configuration authentication mode is encryption algorithm authentication.

【description】

area *area-id* **authentication** The command is used for enarea simple text authentication function.

area *area-id* **authentication message-digest** The command is used for enarea MD5 authentication function.

no area *area-id* **authentication** The command is used for turn off the zone authentication mode function.

In default, the OSPF area authentication method is not configured.

Configuration reference commands **ip ospf authentication-key** and **ip ospf message-digest-key**.

【example】

#Enables the OSPF area 0 for simple text authentication.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#area 0 authentication

32.1.5 ip ospf authentication

【command】

ip ospf authentication [message-digest | null] [*ip-address* **]**

no ip ospf authentication [*ip-address* **]**

【config-mode】

Interface configuration mode

【parameter】

authentication: the configuration interface authentication mode is simple text authentication.

authentication message-digest: The configuration interface authentication method is the encryption algorithm authentication.

authentication null: Not certified.

ip-address: Interface IP address. When there are multiple IP addresses on an OSPF interface, you can specify the authentication method for an interface address separately. When no interface address is specified, all the addresses under the interface use the configured authentication mode.

【description】

ip ospf authentication The command is used for configure the authentication method of the OSPF interface.

no ip ospf authentication The command is used for Unconfigure the configured OSPF interface authentication mode.

By default, the interface authentication mode is not configured.

The OSPF authentication method can be configured on the region, interface, and interface address, with a priority ranging from low to high: region, interface, and interface address. That is, the authentication mode of the interface address is used first, then the interface authentication mode is used, and finally the area authentication mode is used.

【example】

#Configure interface vlan 1 enables encryption algorithm authentication.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf authentication message-digest

32.1.6 ip ospf authentication-key

【command】

ip ospf authentication-key *password [ip-address]*

no ip ospf authentication-key [*ip-address* **]**

【config-mode】

Interface configuration mode

【parameter】

password: Authenticated password, 1-8 character length.

ip-address: Interface IP address. When there are multiple IP addresses on an OSPF interface, you can separately configure an authentication password for an interface address. When the interface address is not specified, all addresses under the

interface use the authentication password.

【description】

ip ospf authentication-key The command is used for configure the interface simple text authentication password.

no ip ospf authentication-key The command is used for Cancel the interface simple text authentication password.

By default, the interface simple text authentication password is not configured.

【example】

#Configuration interface vlan 1 simple text authentication password is 12345678.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf authentication-key 12345678

32.1.7 ip ospf message-digest-key

【command】

ip ospf message-digest-key *key-id* **md5** *password [ip-address]*

no ip ospf message-digest-key *key-id* **[** *ip-address* **]**

【config-mode】

Interface configuration mode

【parameter】

key-id: Key ID, the value range from 1 to 255.

md5 *password*: MD5 authentication password, up to 16 characters.

ip-address: Interface IP address, When there are multiple IP addresses on an OSPF interface, you can specify a separate authentication password for an interface address. When no interface address is specified, all the addresses under the interface use the configured authentication password.

【description】

ip ospf message-digest-key The command is used for configure the interface MD5 authentication password.

no ip ospf message-digest-key The command is used for cancel the interface MD5 authentication password

By default, the MD5 authentication password is not configured.

Notes:

l After the authentication is configured, the OSPF interface needs to authenticate first when receiving the OSPF protocol message, and only when the authentication is passed can it receive the message. Therefore, it is necessary to establish an adjacent OSPF interface, and the authentication mode, Key-ID, and authentication password must be consistent.

【example】

#The MD5 authentication password for the configuration interface vlan 1 is 123456.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf message-digest-key 1 md5 123456

32.1.8 area default-cost

【command】

area *area-id* **default-cost** *cost-value*

no area *area-id* **default-cost**

【config-mode】

OSPF configuration mode

【parameter】

area-id: OSPF area ID, in two ways: one is decimal number between 0 and 42949967295; the other is IP address between 0.0.0.0 and 255.255.255.255.

cost-value: Notice the cost value of the default route, ranging from 0 to 16777214.

【description】

area *area-id* **default-cost** The command is used for configure the Stub region or NSSA region ABR to generate cost values for the default route.

no area *area-id* **default-cost** The command is used for restore the default situation.

By default, the Stub region, the NSSA region ABR generates the default route with a cost value of 1.

After you configure the Stub region, the fully NSSA region, the ABR of that region automatically generates the default route. The NSSA region ABR does not automatically generate default routes, which can be generated through the default-information originate command.

Related configuration reference commands **area stub** and **area nssa**.

【example】

#Configure the default routing co value of the in stub region 1 is 10.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#area 1 stub

Switch(config-router-ospf)#area 1 default-cost 10

32.1.9 default-information originate

【command】

default-information originate [always | metric *metric-value* **| metric-type { 1 | 2 } | route-map** *route-map-name* **]***

no default-information originate [always | metric | metric-type | route-map]*

【config-mode】

OSPF configuration mode

【parameter】

always: Regardless of whether there are default routes in the local route table, the default route is to flood in and external to the OSPF autonomous system.

metric-value: Generate measurements for external default routes, ranging from 0 to 16777214.

metric-type 1: Represents the resulting default route as an internal type.

metric-type 2: Indicates that the generated default route is an external type with a default configuration.

route-map-name: Reenced routing map name, up to 32 characters.

【description】

default-information originate The command is used for configure the flood external default route to the OSPF autonomous system.

no default-information originate The command is used for restore the default situation.

By default, an external default route is not generated to the OSPF autonomous system.

OSPF will not automatically route the flood default to the autonomous system. After the default-information originate command to configure the keyword always, the default route will be forced in the autonomous system. Otherwise, the default route is generated within the OSF autonomous system only if a default route exists locally. This command can specify the metric value or routing type for the default route, or configure a routing policy to flood the default routing when the routing policy conditions are met.

The default route generated by this command is published in Type-5 LSA, which will flood in the entire autonomous system and should be used with caution

【example】

#Force the external default routing to the flood in the OSPF autonomous system.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#default-information originate always

32.1.10 default-metric

【command】

default-metric *metric-value*

no default-metric

【config-mode】

OSPF configuration mode

【parameter】

metric-value: Metric values introducing external routing, ranging from 0 to 16777214, with a default of 20.

【description】

default-metric The command is used for configure the measures that introduce the external routes.

no default-metric The command is used for restore the default situation.

【example】

#Configure the OSPF external routing with a metric value of 30.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#default-metric 30

32.1.11 distance

【command】

distance { *distance [next-hop/length [acl* **]] | ospf { external** *distance* **| inter-area** *distance* **| intra-area** *distance***}* }**

no distance [[*next-hop/length***] | ospf [external | inter-area | intra-area]]**

【config-mode】

OSPF configuration mode

【parameter】

distance: OSPF manages distance, range from 1 to 255, default to 110.

next-hop/length: Next hop address and mask length.

acl: ACL name and ACL number represent the ACL used to match the managed distance of the OSPF route of the upper and down address.

external *distance*: OSPF external route management distance, the value range from 1 to 255.

inter-area *distance*: OSPF interregional route management distance, with values ranging from 1 to 255.

intra-area *distance*: Route ting managed distance within OSPF, ranging from 1 to 255.

【description】

distance The command is used for configure the managed distance for the OSPF routing.

no distance The command is used for restore the default situation.

OSPF route management distance is configured by distance command, with OSPf, which is configured according to OSPF route type, the next hop address OSPF route is configured; that is, all OSPF route management distances are configured

without parameters. When distance distance, distance ospf, and distance distance next-hop are configured simultaneously, distance distance next-hop has the highest priority, distance ospf priority comes second, and distance distance has the lowest priority.

【example】

#Configure the OSPF management distance of 100.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#distance 100

32.1.12 ip ospf bfd

【command】

ip ospf bfd

no ip ospf bfd

【config-mode】

Interface configuration mode

【parameter】

none

【description】

ip ospf bfd The command is used for turn on the BFD function of the OSPF interface.

no ip ospf bfd The command is used for turn off the BFD function of the OSPF interface.

By default, the BFD function of the OSPF interface is not enabled.

【example】

#Configure the interface vlan 1 to open the BFD function.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf bfd

32.1.13 area range

【command】

area *area-id* **range** *ip-address/length* **[cost** *cost-value* **][advertise | not-advertise | substitute** *ip-address/length* **]**

no area *area-id* **range** *ip-address/length* **[substitute]**

【config-mode】

OSPF configuration mode

【parameter】

area-id: OSPF area ID, in two ways: one is decimal number between 0 and 42949967295; the other is IP address between 0.0.0.0 and 255.255.255.255.

ip-address/length: Target network segment and mask length, representing the summarized network address.

cost *cost-value*: Summary value of 0 to 16777215. By default, select the maximum value of the cost in the detail routing.

advertise: Configure the ABR to notify the summary route to other regions. In default, summary routes will be notified to other regions.

not-advertise: Configure ABR does not notify the summary route to other areas.

substitute *ip-address/length*: The summary route uses another network segment instead, with the summary route under the substitute command.

【description】

area *area-id* **range** The command is used for configure the inter-regional routing summary.

no area *area-id* **range** The command is used for cancel the inter-region routing aggregation.

Configure this command on ABR to summarize the routes of a regional network segment, and only notify the summarized routes to other areas, and does not send detailed routes. When the detail route is deleted, the summary route is also automatically deleted.

Notes:

The order only effective on the ABR

【example】

#The summary route for the configured OSPF region 1 is: 1.0.0.0/16, with a cost value of 20 and notification to other areas

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#area 1 range 1.0.0.0/16 cost 20

32.1.14 distribute-list

【command】

distribute-list { *acl-name* | *acl-number* } **out** { **bgp** | **connected** | **isis** | **rip** | **static** }

no distribute-list { *acl-name* | *acl-number* } **out** { **bgp** | **connected** | **isis** | **rip** | **static** }

【config-mode】

OSPF configuration mode

【parameter】

acl-name: The ACL name used for the external route filtering.

acl-number: The ACL number used for the external route filtering.

bgp: BGP routing protocol.

connected: Direct routing protocol.

isis: ISIS routing protocol.

rip: RIP routing protocol.

static: static routing protocol.

【description】

distribute-list The command is used for configure the external routing filtering.

no distribute-list The command is used for cancel the external route filtering function.

By default, the OSPF external routing filtering is not configured.

Configure this command on the ASBR to allow or prohibit the ACL specified OSPF autonomous system to the OSPF autonomous system.

【example】

#Configuration allows the RIP routing of the 1.1.1.0/24 network segments to reissue to the OSPF protocol.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#ip access-list 1 permit 1.1.1.0 0.0.0.255

Switch(config-router-ospf)#distribute-list 1 out rip

32.1.15 area shortcut

【command】

area *area-id* **shortcut { default | disable | enable }**

no area *area-id* **shortcut**

【config-mode】

OSPF configuration mode

【parameter】

area-id: OSPF area ID, in two ways: one is decimal number between 0 and 42949967295; the other is IP address between 0.0.0.0 and 255.255.255.255.

default: default mode.

disable: disable function.

enable: Enable function.

【description】

area *area-id* **shortcut** The command is used for the shortcut mode for the configuration region.

no area *area-id* **shortcut** The command is used for restore the default situation.

OSPF area configuration **shortcut** mode, first configure ABR-Type type: shortcut, refer to command: **ospf abr-type**.

【example】

#The shortcut mode for configuring the OSPF region 1 is: enable

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#area 1 shortcut enable

32.1.16 area nssa

【command】

area *area-id* **nssa [translate-always | translate-candidate | translate-never] [no-summary]**

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

【config-mode】

OSPF configuration modek

【parameter】

area-id: OSPF area ID, in two ways: one is decimal number between 0 and 42949967295; the other is IP address between 0.0.0.0 and 255.255.255.255.

translate-always: Configure the ABR of the NSSA region to force the LSA type transformation.

translate-candidate: decide whether to conduct LSA type conversion according to the election rules between NSSA region ABR.

translate-never: Configure the ABR of the NSSA region to enforce no LSA type conversion.

no-summary: Block interregional routing into the NSSA areas, namely the configured fully NSSA area. When this command is configured, the ABR of the NSSA area produces a default route (Type-3 LSA) notification to the NSSA area, and the devices in the NSSA area reach the destination outside the area by the default route. This parameter is valid only on the ABR.

【description】

area *area-id* **nssa** The command is used for configure the region as the NSSA region.

area *area-id* **nssa no-summary** The command is used for configure the full NSSA region.

no area *area-id* **nssa** The command is used for restore the default situation.

By default, the OSF region does not belong to the NSSA region.

The NSSA region, which does not allow Type-5 LSA injection but allows Type-7 LSA injection, the ABR of the NSSA region

will convert Type-7 LSA to Type-5 LSA and flood these converted Type-5 LSA flooding to the entire autonomous system. When there are multiple ABR in the NSSA region, convert Type-7 LSA to Type-5 LSA by Router ID large ABR by default.

Introduce external routing to the NSSA region by configuring redistribution, and the ASBR of the NSSA region generates a Type-7 LSA and floods into this NSSA region. The ABR in the NSSA region returns Type-7 LSA to Type-5 LSA and floods these converted Type-5 LSA to the entire autonomous system.

Notes:

l The backbone region cannot be configured as an NSSA region.

l All devices in the same NSSA region must be configured as NSSA regions between devices with inconsistent region types.

【example】

#Configure region 1 for the NSSA region

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#area 1 nssa

32.1.17 area stub

【command】

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

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

【config-mode】

OSPF configuration mode

【parameter】

area-id: OSPF area ID, in two ways: one is decimal number between 0 and 42949967295; the other is IP address between 0.0.0.0 and 255.255.255.255.

no-summary: Configure a fully stub area to block inter-zone routes and external routes from entering this area. This parameter is valid only on the ABR.

【description】

area *area-id* **stub** The command is used for configure the region as stub region.

area *area-id* **stub no-summary** The command is used for configure regions as full stub regions.

no area *area-id* **stub** The command is used for restore the default situation.

By default, the OSPF region is not part of the stub region.

The OSPF Stub area does not allow AS external routes to flood within the area, and the full Stub area does not allow AS external routes for flooding within the area。

Notes:

The backbone region cannot be configured as a stub region.

All devices in the same stub region must be configured as stub regions, and devices with inconsistent region types cannot form neighbors.

【example】

#Configure area 1 as the stub region

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#area 1 stub

32.1.18 area virtual-link

【command】

area *transit-area-id* **virtual-link** *neighbor-id* **[authentication-key** *key* **| message-digest-key** *key-id* **md5** *key* **]** **[dead-interval** *seconds***] [hello-interval** *seconds***] [retransmit-interval** *seconds***] [transmit-delay** *seconds* **]**

no area *transit-area-id* **virtual-link** *neighbor-id*

【config-mode】

OSPF configuration mode

【parameter】

transit-area-id: Transmission area ID through which the virtual link passes.

neighbor-id: Virtual link link Router ID of the paired-end device.

authentication-key *key*: Simple text authentication authentication password, up to 8 characters.

message-digest-key *key-id*: MD5 certified key id, the value range is from 1 to 255.

md5 *key*: MD5 certified password, up to 16 characters.

dead-interval *seconds*: Neighborhood failure time, in seconds, ranged from 1 to 65535, with a default value of 40 seconds.

hello-interval *seconds*: Send a Hello time interval in seconds and range from 1 to 65535 with a default value of 10 seconds.

retransmit-interval *seconds*: LSA retransmission interval, in seconds, range from 1 to 65535 with a default of 5 seconds.

transmit-delay *seconds*: LSA transmission delay in seconds, value range from 1 to 65535, default value is 1 second.

【description】

area *transit-area-id* **virtual-link** The command is used for configuring the virtual links.

no area *transit-area-id* **virtual-link** The command is used for cancel the false link.

Non-backbone regions in OSPF must complete the synchronization of database and data interaction. Therefore, it is required that all the non-backbone regions must remain connected to the backbone regions. When this requirement, logical connectivity can be established by configuring virtual links.

Notes:

The virtual link must be configured between the two ABRs

The two ABRs configured the virtual link must be in the same common area, which is called the virtual link transfer area (Transit Area).

The linked transport area cannot be the Stub areas and the NSSA areas.

【example】

#Configure a virtual link between dut1 and dut2 with a transmission area of 1

#Configuration of the device dut1

dut1#configure terminal

dut1(config)#router id 1.1.1.1

dut1(config)#router ospf

dut1(config-router-ospf)#area 1 virtual-link 2.2.2.2

#Configuration of the device dut2

dut2#configure terminal

dut2(config)#router id 2.2.2.2

dut2(config)#router ospf

dut2(config-router-ospf)#area 1 virtual-link 1.1.1.1

32.1.19 area filter-list

【command】

area *area-id* **filter-list prefix** *prefix-name* **{ in | out }**

no area *area-id* **filter-list prefix** *prefix-name* **{ in | out }**

【config-mode】

OSPF configuration mode

【parameter】

area-id: OSPF area ID, in two ways: one is decimal number between 0 and 42949967295; the other is IP address between 0.0.0.0 and 255.255.255.255.

prefix-name: Filter the prefix list name.

in: ABR filters using the prefix list when receiving Type-3 LSA notified from other areas.

out: ABR uses the prefix list to filter when notifying Type-3 LSA to other areas.

【description】

area *area-id* **filter-list** The command is used for configure inter-region routing filtering.

no area *area-id* **filter-list** The command is used for cancel the inter-regional route filtering.

By default, the routes are not filtered.

Only prefix list filtering is supported.

ABR uses the in in direction filtering when receiving inter-region routing list, and the out direction filtering when announcing inter-region routing.

【example】

#When configure ABR the Type-3 LSA to notify area 1 to other areas, match Prefix-list aa: notify only the route 10.1.1.0/24.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#ip prefix-list aa permit 10.1.1.0/24

Switch(config-router-ospf)#area 1 filter-list prefix aa out

32.1.20 auto-cost reference-bandwidth

【command】

auto-cost reference-bandwidth *reference-bandwidth*

no auto-cost reference-bandwidth

【config-mode】

OSPF configuration mode

【parameter】

reference-bandwidth: Reference bandwidth in Mbit/s, range from 1 to 4294967.

【description】

auto-cost reference-bandwidth The command is used for configure the reference bandwidth values.

no auto-cost reference-bandwidth The command is used for restore the default situation.

By default, the reference bandwidth is 100 Mbit/s.

The reference bandwidth is used to calculate the cost value of the OSPF interface (cost= reference bandwidth / physical bandwidth of the interface). If the calculation result is greater than 1, the integer part is taken; if less than 1,1 is taken.

【example】

#The reference bandwidth for the configured OSPF is 1,000 Mbit/s.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#auto-cost reference-bandwidth 1000

32.1.21 bandwidth

【command】

bandwidth *bandwidth-value*

no bandwidth

【config-mode】

Vlan interface configuration mode

【parameter】

bandwidth-value: Interface bandwidth value, in k bit/s, values range from 1 to 10000000.

【description】

bandwidth *bandwidth-value* The command is used for configure the interface bandwidth value.

no bandwidth The command is used for remove the configuration.

By default, the reference bandwidth is 10 Mbit/s.

【example】

#The bandwidth of the configured vlan 2 interface is 1000 Mbit/s.

Switch#configure terminal

Switch(config)#interface vlan-interface 2

Switch(config-if-vlanInterface-2)#hbandwidth 1000000

32.1.22 capability opaque

【command】

capability opaque

no capability opaque

【config-mode】

OSPF configuration mode

【parameter】

none

【description】

capability opaque The command is used for Configure the OSPF to support the Opaque LSA.

no capability opaque The command is used for cancel the OSPF Opaque LSA function.

By default, the OSPF does not support the Opaque LSA functionality.

Opaque LSA Mainly used in the OSPF GR, OSPF TE environment.

【example】

#Configure the OSPF to support the Opaque LSA.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#capability opaque

32.1.23 ip ospf cost

【command】

ip ospf cost *cost-value [ip-address]*

no ip ospf cost *[ip-address]*

【config-mode】

interface configuration mode

【parameter】

cost-value: OSPF routing measures, ranging from 1 to 65535.

ip-address: Interface IP address, when there are multiple IP addresses on an OSPF interface, you can separately configure the routing measures for certain addresses of the interface.

【description】

ip ospf cost The command is used for configure the interface measure value.

no ip ospf cost The command is used for restore default situation.

By default, the cost value under the OSPF interface is 10.

【example】

#The configuration interface vlan 1 has a cost value of 100.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf cost 100

32.1.24 ip ospf dead-interval

【command】

ip ospf dead-interval { *dead-value* **| minimal hello-multiplier** *number } [ip-address]*

no ip ospf dead-interval [*ip-address* **]**

【config-mode】

Interface configuration mode

【parameter】

dead-value: The OSPF neighbor failure time, in seconds, ranged from 1 to 65535, with a default value of 40s.

minimal: The aging time for the configured OSPF neighbors is min: 1s.

hello-multiplier *number*: Configure the number of hello messages sent within 1 second to range from 1 to 10.

ip-address: Interface IP address, when there are multiple IP addresses on an OSPF interface, you can separately configure the neighbor expiration time on certain addresses.

【description】

ip ospf dead-interval The command is used for configure the OSPF neighbor failure time.

no ip ospf dead-interval The command is used for restore default situation.

By default, the OSPF neighbor failure time is 4 times the Hello time interval, namely 40 seconds in broadcast and P2P networks and 120 seconds in P2MP and NBMA networks.

【example】

#The OSPF neighbor failure time of the configured interface vlan 1 is 30 seconds.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf dead-interval 30

32.1.25 ip ospf hello-interval

【command】

ip ospf hello-interval *hello-value [ip-address]*

no ip ospf hello-interval *[ip-address]*

【config-mode】

Interface configuration mode

【parameter】

hello-value: The interval between OSPF sending Hello messages ranges from 1 to 255 (seconds).

ip-address: Interface IP address, when there are multiple IP addresses on an OSPF interface, you can separately configure the neighbor Hello time on certain addresses.

【description】

ip ospf hello-interval The command is used for configure the interval between OSPF sending Hello messages.

no ip ospf hello-interval The command is used for restore the default situation.

In default, the time interval of OSPF sending Hello messages is determined by network type, 10 seconds in broadcast network and P2P network and 30 seconds in P2MP and NBMA network.

Neighbor failure time configuration reference command ip ospf dead-interval.

Notes:

The Hello time interval and the neighbor failure time must be consistent between the OSPF adjacent devices, otherwise the neighbor relationship cannot be established.

By default, the neighbor failure time is 4 times the Hello time interval.

Modify the Hello time interval, if the current neighbor failure time is 4 times the Hello time interval, the neighbor failure time is automatically modified to maintain 4 times relationship; if the current neighbor failure time is not 4 times the Hello time interval, the neighbor failure time remains unchanged.

Modifying the neighbor failure time does not affect the Hello time interval.

【example】

#The OSPF Hello message sending interval of the configured interface vlan 1 is 20 seconds.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf hello-interval 20

32.1.26 ip ospf mtu-ignore

【command】

ip ospf mtu-ignore [*ip-address* **]**

no ip ospf mtu-ignore [*ip-address* **]**

【config-mode】

Interface configuration mode

【parameter】

ip-address: Interface IP address, when there are multiple IP addresses on an OSPF interface, the neighbors of some addresses of the interface can ignore the MTU consistency check separately.

【description】

ip ospf mtu-ignore The command is used for enignore MTU consistency check during DD interaction.

no ip ospf mtu-ignore The command is used for restore the default situation.

By default, check the MTU consistency, if not, do not form a neighbor relationship.

【example】

#MTU consistency checks at interface vlan 1.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf mtu-ignore

32.1.27 ip ospf network

【command】

ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ip ospf network

【config-mode】

Interface configuration mode

【parameter】

broadcast: Indicates that the configuration OSPF interface type is a broadcast type, with the default configuration.

non-broadcast: Indicates that the configuration OSPF interface type is an NBMA.

point-to-multipoint: Indicates that the configuration OSPF interface type is P2MP.

point-to-point: Indicates that the configuration OSPF interface type is a P2P.

【description】

ip ospf network The command is used for configure the OSPF interface network type.

no ip ospf network The command is used for restore the default situation.

By default, the OSPF network type is determined by the link layer protocol:

Broadcast network —— When the link protocol is Ethernet, FDDI, the OSPF default network type is broadcast.

P2P (Point To Point Network) —— When the link protocol is PPP, LAPB, and HDLC, the OSPF default network type is P2P.

NBMA network (Non-Broadcast Multi-Access Network, NBMA) —— When the link protocol is an ATM, frame relay, or X.25, the OSPF default network type is an NBMA.

P2MP (Point To Multi-Point Network) —— No link protocol is considered P2MP type by OSPF default, and the not fully connected NBMA network is usually configured as OSPF P2MP network.

Notes:

The interface network type of the ospf neighbor must be consistent, otherwise the neighbor establishment is unsuccessful or the routing calculation fails.

【example】

#The network type for the configured interface vlan 1 is P2P.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf network point-to-point

32.1.28 ip ospf priority

【command】

ip ospf priority *priority-value [ip-address]*

no ip ospf priority *[ip-address]*

【config-mode】

Interface configuration mode

【parameter】

priority-value: Configure the priority of the OSPF interface to range from 0 to 255.

ip-address: Interface IP address, when there are multiple IP addresses on an OSPF interface, you can configure the priority of some addresses of the interface separately.

【description】

ip ospf priority The command is used for configure the OSPF interface priority.

no ip ospf priority The command is used for restore the default situation.

By default, the OSPF interface priority is 1.

Interface priority is mainly used for broadcast network, NBMA network, designated router DR (Designed Router), backup specified router BDR (Backup Designed Router) election, the greater the value, the higher the priority. Priority is 0, do not participate in the election.

Notes:

Priority only affects the election process. When DR and BDR have been elected in the network, modifying the interface priority will not affect the election result and only affects the election result of the next DR or BDR. Therefore, DR is not necessarily the device with the highest interface priority, and BDR is not necessarily the device with the second highest interface priority.

【example】

#The configuration interface vlan 1 has a priority of 100.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf priority 100

32.1.29 ip ospf retransmit-interval

【command】

ip ospf retransmit-interval *interval-value [ip-address]*

no ip ospf retransmit-interval *[ip-address]*

【config-mode】

Interface configuration mode

【parameter】

interval-value: Time interval of retransmitted LAS, with values ranging from 1 to 65535 in seconds.

ip-address: Interface IP address, when there are multiple IP addresses on an OSPF interface, retransmission intervals can be configured separately for an interface address. When no interface address is specified, all addresses under the interface use the configured retransmission interval.

【description】

ip ospf retransmit-interval The command is used for configure the interface LAS retransmission time interval.

no ip ospf retransmit-interval The command is used for restore the default situation.

By default, the retransmission time interval is 5 seconds.

【example】

#The retransmission interval of the configuration interface vlan 1 is 10 seconds.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf retransmit-interval 10

32.1.30 ip ospf transmit-delay

【command】

ip ospf transmit-delay *delay-value [ip-address]*

no ip ospf transmit-delay *[ip-address]*

【config-mode】

Interface configuration mode

【parameter】

delay-value: The retransmission interval of the configuration interface vlan 1 is 10 seconds.

ip-address: Interface IP address, When there are multiple IP addresses on an OSPF interface, the transfer delay can be configured separately for an interface address. When no interface address is specified, all addresses under the interface use the configured transfer delay.

【description】

ip ospf transmit-delay The command is used for configure the interface LAS retransmission time interval.

no ip ospf transmit-delay The command is used for restore the default situation.

By default, the LSA transmission delay is 1 second.

The LSA transmission delay indicates the time taken for the LSA to flood to other devices, and the LSA sender adds the interface transmission delay to the aging time of the LSA to be sent.

【example】

#The transmission delay of the configuration interface vlan 1 is 60 seconds.

Switch#configure terminal

Switch(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip ospf transmit-delay 60

32.1.31 log-adjacency-changes

【command】

log-adjacency-changes [detail]

no log-adjacency-changes [detail]

【config-mode】

OSPF configuration mode

【parameter】

detail: Displays details of neighbor state changes.

【description】

log-adjacency-changes The command is used for enables to record OSPF neighbor state changes.

no log-adjacency-changes The command is used for cancel the enabling function.

By default, the OSPF neighbor status changes are not recorded.

【example】

#Turn on the recording OSPF neighbor state change function.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#log-adjacency-changes detail

32.1.32 neighbor

【command】

neighbor *ip-address* **[poll-interval** *seconds* **| priority** *priority-value* **]**

no neighbor *ip-address* **[poll-interval** *seconds* **| priority** *priority-value* **]**

【config-mode】

OSPF configuration mode

【parameter】

ip-address: Interface IP address of the neighbor.

poll-interval *seconds*: When the neighbor state is down, the interval between sending hello messages ranges from 1 to 65535, with a default value of 60 seconds.

priority *priority-value*: Priority, value range 0-255, the priority configured here will not affect the choice of DR and BDR, configuration and no configuration is no effect, DR and BDR selection is based on the priority of the interface vlan, configuration interface priority command please refer to: **ip ospf priority**.

【description】

neighbor The command is used for configure the neighbors in the NBMA network.

no neighbor The command is used for restore the default situation.

By default, neighbors are not automatically found in the NBMA network.

【example】

#Configure the neighbors in the NBMA network.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#neighbor 1.1.1.1

32.1.33 ospf abr-type

【command】

ospf abr-type { cisco | ibm | shortcut | standard }

no ospf abr-type

【config-mode】

OSPF configuration mode

【parameter】

cisco: Represents the Cisco device ABR performance, with the default configuration.

ibm: Represents the IBM device ABR representation.

shortcut: ABR is expressed in shortcut mode.

standard: Represents the presentation mode as specified by the RFC2328.

【description】

ospf abr-type The command is used for configure how OSPF ABR behave.

no ospf abr-type The command is used for restore default situation.

By default, the ABR is represented as Cisco.

ABR meets different conditions under different criteria:

Cisco and IBM: Two or more regions are connected, and one region is a backbone region.

Shortcut and Standard: Two or more areas are connected.

【example】

#Configuration OSPF ABR performs consistently with Standard.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#ospf abr-type standard

32.1.34 ospf rfc1583 compatibility

【command】

ospf rfc1583compatibility

no ospf rfc1583compatibility

【config-mode】

OSPF configuration mode

【parameter】

None

【description】

ospf rfc1583compatibility The command is used for enables compatibility with the rules in the RFC1583.

no ospf rfc1583compatibility The command is used for restore default situation.

Incompatible, RFC1583 in default.

OSPF may calculate external routing due to inconsistent routing calculation rules between RFC2328 and RFC1583. To avoid the routing loop, the RFC1583 compatibility feature is proposed in RFC2328.

After enabling RFC1583 compatibility, OSPF adopts RFC1583 routing calculation rules.

When RFC1583 is not compatible, OSPF uses RFC2328.

【example】

#Configure that the OSPF is compatible with the RFC1583.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#ospf rfc1583compatibility

32.1.35 passive-interface

【command】

passive-interface { **default** | **supervlan-interface** *interface-id [ip-address]* | **vlan-interface** *interface-id [ip-address] }*

no passive-interface { **default** | **supervlan-interface** *interface-id [ip-address]* | **vlan-interface** *interface-id [ip-address] }*

【config-mode】

OSPF configuration mode

【parameter】

default: The default passive interface means that all interfaces are configured as passive interfaces.

supervlan-interface *interface-id*: Supervlan Take the slogan, the value range is 1~128.

vlan-interface *interface-id*: Vlan takes the slogan, and the value range is from 1 to 4094.

ip-address: Interface IP address, separately specified that some addresses of the interface are passive interface.

【description】

passive-interface The command is used for configure the OSPF passive interface.

no passive-interface The command is used for cancel the OSPF passive interface.

The OSPF interface is not passive interface by default.

After the OSPF passive interface is configured, it can notify the route of the direct network segment where the interface is located through the network command, but suppress the reception and transmission of OSPF protocol messages on the interface.

【example】

#Configure the vlan 2 interface as a passive interface.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#passive-interface vlan-interface 2

32.1.36 redistribute

【command】

redistribute { bgp | connected | isis | rip | static } [metric *metric-value* **| metric-type { 1 | 2 } | route-map** *route-map-name* **]***

no redistribute { bgp | connected | isis | rip | static } [metric | metric-type | route-map]*

【config-mode】

OSPF configuration mode

【parameter】

bgp: The BGP routing.

connected: Direct routing.

isis: The ISIS routing.

rip: The RIP routing.

static: Static routing.

metric *metric-value*: Specifies the redistribution routing metric value, ranging from 0 to 16777214.

metric-type { 1 | 2 }: Specifies the type of redistribution route, value external type 1 or external type 2 and default external type 2.

route-map *route-map-name*: Routing policy name, configure routing policies for routing control when redistributing routing.

【description】

redistribute The command is used for redistribution of the external routing for the OSPF.

no redistribute The command is used for cancel the OSPF redistribute external routing function.

In default, there is no external route redistributed. Route redistribution route flooding from other routing protocols to the OSPF autonomous system.

When the multiple routing protocols are running on a device, the routing of the other protocols are introduced into the OSPF autonomous system through redistribution, the default generates the OSPF second type of external routing with a routing metric value of 20. When redistribution introduces external routing, you can modify the external routing types and metric and metric-type fields, and configure the corresponding routing policy for route control and management.

【example】

#The redistribution rip protocol routes to the OSPF domain and specifies a redistribution metric value of 30 and the routing type of the external type 2.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#redistribute rip metric 30 metric-type 2

32.1.37 refresh timer

【command】

refresh timer *time-value*

no refresh timer

【config-mode】

OSPF configuration mode

【parameter】

time-value: Scan time, with values ranging from 10 to 1800 in seconds.

【description】

refresh timer The command is used for configure the OSPF scan time interval.

no refresh timer The command is used for restore default value.

By default, the scan time is 10 seconds, and any LSA refreshes in the OSF time scan database.

【example】

#Configure the OSPF scan time for 30 seconds.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#refresh timer 30

32.1.38 timers throttle spf

【command】

timers throttle spf *delay-time hold-time max-time*

no timers throttle spf

【config-mode】

OSPF configuration mode

【parameter】

delay-time: Initial delay was calculated with values ranging from 0 to 600000 ms.

hold-time: Inhibition time, with values ranging from 0 to 600000 ms.

max-time: Maximum waiting time for two SPF calculations, with values ranging from 0 to 600000 ms.

【description】

timers throttle spf The command is used for configure the time parameters for the SPF calculation.

no timers throttle spf The command is used for restore default value.

By default, the initial delay delay is 2000 ms, the suppression time hold-time is 4000 ms, and the maximum waiting time max-time for two SPF calculations is 10000 ms.

【example】

#The SPF calculation started 3000 ms after receiving the topology change with a suppression time of 5000 ms and a maximum waiting time of 20000 ms.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#timers throttle spf 3000 5000 20000

32.2 OSPF Monitoring and debugging commands

32.2.1 show ip ospf neighbor

【command】

show ip ospf [*process-id* **] neighbor**

【config-mode】

Any configuration mode

【parameter】

process-id: Process number of the OSPF, with the value range from 1 to 10.

【description】

show ip ospf neighbor The command is used for display the neighbor information for the OSPF.

【example】

#Display the neighbor information for the OSPF.

Switch#show ip ospf neighbor

Type: D - Dynamic, S - Static

Type	Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtL	RqstL	DBsmL
D	2.2.2.2	1	Full/Backup	36.660s	10.1.1.2	VLAN-IF10	0	0	0

show ip ospf neighbor field description

Field	Description
Type	The type of neighbor: D: Dynamic neighbor S: Static neighbor
Neighbor ID	The Router ID of the neighbor device
Pri	Priority of the neighbor devices
State	Status of the neighbor / interface role; Status of the neighbors, including: Down -- the initial state of the neighbor session. Attempt -- When the DR-qualified device in the NBMA network connects to its neighbor becomes valid, the neighbor state is set to Attempt, which is only valid for the neighbor on the NBMA network. Init -- receives a Hello message from its neighbors, but the neighbor field in the Hello message does not contain its own Router ID. Way -- saw his own RouterID in a Hello message received by his neighbors, indicating that two-way communication is established. Exstart -- Establish the master / slave relationship between the equipment and the neighbor, determine the serial number of the DD message, and prepare for the exchange of the DD message. Exchange -- The device sends a DD message to its neighbor describing its entire link status database information.

	Loading -- The device sends a link status request message to its neighbor to request the latest LSA. Full -- Establish complete full ency between device and neighbors. The role of devices in broadcast, NBMA networks, including: DR -- Specify a router (Designate Router), which only exists in broadcast, NBMA networks. BDR -- Backup the specified router (Buckup Designate Router), present only in broadcast, NBMA networks. DRother -- All equipment in the broadcast and NBMA network except DR and BDR In the P2P and P2MP networks, the role appears as: DROther.
Dead Time	Time of failure of neighbors
Address	Interface IP address of the neighbor device
Interface	Interface connected to the network where the neighbor device is located
RXmtL	The LSA quantity statistics on the retransmission list
RqstL	The LSA quantity statistics on the request list
DBsmL	Database summary list: LSA quantity statistics

32.2.2 show ospf route-table

【command】

show ip ospf [*process-id* **] route-table**

【config-mode】

Any configuration mode

【parameter】

process-id: Process number of the OSPF, with the value range from 1 to 10.

【description】

show ospf route-table The command is used for displays the routing table information for the OSPF.

【example】

#Displays the routing table information for the OSPF.

```
Switch(config-router-ospf)#show ospf route-table

============ OSPF network routing table ============

N       10.1.1.0/24                 [10] area: 0.0.0.0

                                        directly attached to VLAN-IF10

N IA 50.1.1.0/24                [20] area: 0.0.0.0

                                        via 10.1.1.1, VLAN-IF10

N       192.168.1.0/24              [10] area: 0.0.0.0

                                        directly attached to VLAN-IF1


============ OSPF external routing table ============

N E2 3.0.0.0/24                 [20/20] tag: 0

                                        via 10.1.1.1, VLAN-IF10

N E2 3.0.1.0/24                 [10/20] tag: 0

                                        via 10.1.1.1, VLAN-IF10

N E2 33.1.1.0/24                [20/20] tag: 0

                                        via 10.1.1.1, VLAN-IF10
```

show ospf route-table field description

Field	Description

OSPF network routing table	OSPF Internal routing
OSPF external routing table	OSPF External routing
IA	OSPF interregional routing
10.1.1.0/24	The purpose of the routing network
[10]	The overhead value of the route
area	Area where the route is located
directly attached to VLAN-IF10	Direct connection routing and corresponding interfaces
E1	External type of OSPF, metric-type type 1, including (class 5 and 7 LSA)
E2	External type of OSPF, metric-type type 2, including (class 5 and 7 LSA)
[20/20]	The previous 20 represents the internal overhead value of the routing, and the following 20 represents the external overhead value of the routing
tag	Marking for the external routing
via 10.1.1.1, VLAN-IF10	The next hop address of the route and the corresponding exit interface

32.2.3 show ip ospf

【command】

show ip ospf [*process-id***]**

【config-mode】

Any configuration mode

【parameter】

process-id: Process number of the OSPF, with the value range from 1 to 10.

【description】

show ip ospf The command is used for displays the OSPF process information and the parameters.

【example】

#View the information about the OSPF.

Switch#show ip ospf

OSPF Routing Process, Router ID: 192.168.1.1

Supports only single TOS (TOS0) routes

This implementation conforms to RFC2328

RFC1583Compatibility flag is disabled

OpaqueCapability flag is disabled

Initial SPF scheduling delay 2000 millisec(s)

Minimum hold time between consecutive SPFs 4000 millisec(s)

Maximum hold time between consecutive SPFs 10000 millisec(s)

Hold time multiplier is currently 2

SPF algorithm last executed 1h31m18s ago

SPF timer is inactive

Refresh timer 10 secs

Number of external LSA 0. Checksum Sum 0x00000000

Number of opaque AS LSA 0. Checksum Sum 0x00000000

Number of areas attached to this router: 1

Area ID: 0.0.0.0 (Backbone)

Number of interfaces in this area: Total: 1, Active: 1

Number of fully adjacent neighbors in this area: 1

Area has no authentication

SPF algorithm executed 9 times

Number of LSA 3

Number of router LSA 2. Checksum Sum 0x00008384

Number of network LSA 1. Checksum Sum 0x00006ad5

Number of summary LSA 0. Checksum Sum 0x00000000

Number of ASBR summary LSA 0. Checksum Sum 0x00000000

Number of NSSA LSA 0. Checksum Sum 0x00000000

Number of opaque link LSA 0. Checksum Sum 0x00000000

Number of opaque area LSA 0. Checksum Sum 0x00000000

show ip ospf field description

Field	Description
OSPF Routing Process, Router ID	The Router ID of the OSPF
This implementation conforms to RFC2328	Implement according to the RFC2328
RFC1583Compatibility flag is disabled	Compatible with the RFC1583 enabling state
OpaqueCapability flag is disabled	Flag enabling state supporting Opaque LSA
Initial SPF scheduling delay 2000 millisec(s)	Initial SPF calculation time delay
Minimum hold time between consecutive SPFs 4000 millisec(s)	The SPF calculated the inhibition time
Maximum hold time between consecutive SPFs 10000 millisec(s)	Maximum time interval for the SPF calculation

Hold time multiplier is currently	Hold time Multiples of the time
SPF algorithm last executed 1h31m18s ago	Time when the last run was SPF calculated
SPF timer is inactive	The SPF timer status
Refresh timer 10 secs	Timed scan database has the LSA scan time to refresh
Number of external LSA	Number of external LSA
Number of opaque AS LSA	The number of the opaque AS LSA
Number of areas attached to this router:	Number of areas on the device
Number of interfaces in this area: Total: 1, Active: 1	Number of interfaces covered by area, Total number of interfaces, Active number of active interfaces
Number of fully adjacent neighbors in this area: 1	Number of neighbors in the FULL state
Area has no authentication	Whether the area opens the authentication
SPF algorithm executed 2 times	Number of times the SPF calculations were run

32.2.4 show ip ospf border-routers

【command】

show ip ospf [*process-id* **] border-routers**

【config-mode】

Any configuration mode

【parameter】

process-id: Process number of OSPF, the value range from 1 to 10.

【description】

show ip ospf border-routers The command is used for show OSPF routes to the ABR or ASBR.

【example】

#View the OSPF routing information up to the ABR or the ASBR.

Switch#show ip ospf border-routers

========== OSPF router routing table ==========

R 192.0.0.4 [10] area: 0.0.0.0, ABR, ASBR

via 70.1.1.2, VLAN-IF70

R 192.0.0.5 [10] area: 0.0.0.1, ABR

via 80.1.1.2, VLAN-IF80

show ip ospf border-routers field description

Field	Description
R 192.0.0.4	The Route ID of ABR or ASBR
[10]	Route the metric-values
area	Area where the interface is located
ABR, ASBR	ASBR: Route to the ASBR ABR: Route to the ABR
via 70.1.1.2	Route the next hop interface address
VLAN-IF70	Routing out interface

32.2.5 show ip ospf database

【command】

show ip ospf [*process-id* **] database [asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary]**

【config-mode】

Any configuration mode

【parameter】

process-id: Process number of OSPF, the value range from 1 to 10.

asbr-summary: Represents the OSPF Type-4 LSA in the display database.

external: Represents the OSPF Type-5 LSA in the display database.

network: Represents the OSPF Type-2 LSA in the display database.

nssa-external: Represents the OSPF Type-7 LSA in the display database.

opaque-area: Represents the OSPF Type-8 LSA in the display database.

opaque-as: Represents the OSPF Type-9 LSA in the display database.

opaque-link: Represents the OSPF Type-10 LSA in the display database.

router: Represents the OSPF Type-1 LSA in the display database.

summary: Represents the OSPF Type-3 LSA in the display database.

【description】

show ip ospf database The command is used for displays the OSPF database information

【example】

#View the OSPF database information.

Switch#show ip ospf database

Router Link States (Area 0.0.0.0)

Link ID ADV Router Age Seq# CkSum Link count

2.2.2.2 2.2.2.2 586 0x80000042 0x6478 1

192.168.1.1 192.168.1.1 470 0x80000041 0x1403 1

Net Link States (Area 0.0.0.0)

Link ID ADV Router Age Seq# CkSum

10.1.1.2 2.2.2.2 386 0x80000006 0x8f3c

Summary Link States (Area 0.0.0.0)

Link ID ADV Router Age Seq# CkSum Route

1.0.0.0 192.168.1.1 390 0x80000004 0xad35 1.0.0.0/24

50.1.1.0 192.168.1.1 950 0x80000004 0x0da3 50.1.1.0/24

ASBR-Summary Link States (Area 0.0.0.0)

Link ID ADV Router Age Seq# CkSum

193.0.0.2 192.168.1.1 240 0x80000004 0xb768

show ip ospf database field description

Field	Description
Router Link States	OSPF LSA Type is Router-LSA, and the LSA in OSPF mainly includes: Type-1 LSA—Router LSA Type-2 LSA—Network LSA Type-3 LSA—Summary LSA Type-4 LSA—Summary ASBR LSA

	Type-5 LSA —AS External LSA Type-7 LSA—NSSA External LSA
Link ID	The link state ID of the LSA
ADV Router	The LSA's advertisement router
Age	Aging time of the LSA
Seq#	Serial number of the LSA
CkSum	Checksum of the LSA
Link count	Number of link information carried in the Type-1 LSA
Route	Routing information carried by Type-3 LSA, Type-5 LSA, and Type-7 LSA

32.2.6 show ip ospf interface

【command】

show ip ospf [*process-id*] **interface** [**supervlan-interface** *interface-id* | **vlan-interface** *interface-id*]

【config-mode】

Any configuration mode

【parameter】

process-id: Process number of the OSPF, with the value range from 1 to 10.

supervlan-interface *interface-id*: supervlan Interface, taking the value range from 1 to 128.

vlan-interface *interface-id*: The vlan interface, the value range is 1 to 4094.

【description】

show ip ospf interface The command is used for displays the interface information for the OSPF.

【example】

#Displays the interface information for the OSPF.

Switch#show ip ospf interface

OSPF status and config information.

area IP address DR BDR state type

0.0.0.0 10.1.1.1 10.1.1.2 10.1.1.1 Backup BROADCAST

pri cost HInterval DInterval ReTrInterval TrDelay

1 10 10s 40s 5s 1s

status auth key-id auth-key

active N/A N/A N/A

area IP address DR BDR state type

0.0.0.1 50.1.1.1 50.1.1.1 none DR BROADCAST

pri cost HInterval DInterval ReTrInterval TrDelay

1 10 10s 40s 5s 1s

status auth key-id auth-key

active N/A N/A N/A

show ip ospf interface field description

Field	Description
area	Area where the interface is located
IP address	The IP address of the interface
DR	Interface IP address of the DR

BDR	Interface IP address of the BDR
state	The state of the interface has three states: DR, Backup, and DROther
type	Network type
pri	Interface priority
cost	Interface cost value
HInterval	The interval between the interface sends the hello message
DInterval	Aging time of the neighbors
ReTrInterval	Interval time between the retransmitted LSA
TrDelay	Delay time of the LSA
status	The state of the interface, there are two kinds active: Active interface, capable of sending and receiving OSPF protocol messages passive: Passive interface, cannot send or receive the OSPF protocol message
auth	The authentication method of the interface supports two authentication methods: simple: Simple text authentication method Md5: MD5 certification method N/A: Certification is not opened
key-id	MD5 Certified Key-id

auth-key	Certified password

32.2.7 show ip ospf virtual-link

【command】

show ip ospf [*process-id*] virtual-link

【config-mode】

Any configuration mode

【parameter】

process-id: Process number of the OSPF, with the value range from 1 to 10.

【description】

show ip ospf virtual-link The command is used for display the virtual link information for the OSPF.

【example】

#Display the virtual link information for the OSPF.

Switch#show ip ospf virtual-link

OSPF vritual link information.

area neighbor HInterval DInterval ReTrInterval

0.0.0.1 2.2.2.2 10 40 5

TrDelay auth auth-key key-id state

1 N/A N/A N/A Point-To-Point

show ip ospf virtual-link field description

Field	Description

area	The virtual link transmission area ID
neighbor	The Router ID of the virtual link neighbor device
HInterval	The interval between the hello message
DInterval	Aging time of the neighbors
ReTrInterval	Retransmission interval time of the LSA
TrDelay	Transmission delay time of the LSA
auth	The authentication method of virtual link supports two authentication methods: simple: Simple text authentication method Md5: MD5 certification method N/A: Certification is not opened
auth-key	Certification password
key-id	MD5 Certified Key-id
state	Network type, and the virtual link is the P2P

32.2.8 debug ospf

【command】

debug ospf

no debug ospf

【config-mode】

Global configuration mode

【parameter】

None

【description】

debug ospf The command is used for open the OSPF debugging master switch.

no debug ospf The command is used for turn off the OSPF debugging master switch.

By default, the OSPF debug master switch is turned off.

【example】

#Open the OSPF debugging master switch.

Switch#configure terminal

Switch(config)#debug ospf

32.2.9 debug ip ospf

【command】

debug ip ospf [*process-id*] { **events** | **ism** [**events** | **status** | **timers**] | **lsa** [**flooding** | **generate** | **install** | **refresh**] | **nsm** [**events** | **status** | **timers**] | **nssa** | **packet** { **all** | **dd** | **hello** | **ls-ack** | **ls-request** | **ls-update** } [**recv** | **send**] | **zebra** [**interface** | **redistribute**] }

no debug ip ospf { **events** | **ism** | **lsa** | **nsm** | **nssa** | **packet** { **all** | **dd** | **hello** | **ls-ack** | **ls-request** | **ls-update** } | **zebra**

【config-mode】

Global configuration mode

【parameter】

process-id: the process number of the OSPF, with the value range from 1 to 10.

events: Indicates the event information debugging switch.

ism: represents the interface status information debugging switch.

status: Represents the status information.

timers: Represents the timer information.

lsa: represents the LSA information debugging switch.

flooding: Represents the LSA flood flood information in the autonomous system.

generate: Represents the information that generates the LSA.

install: Represents the information for installing the LSA.

refresh: Refresh the LSA information.

nsm: represents the neighbor information debugging switch.

nssa: a debug switch for NSSA area information.

packet: Represents the message interaction information debugging switch.

all: indicates all message messages.

dd: represents the database description message interaction information.

hello: means Hello message interaction information.

ls-ack: indicates message message message.

ls-request: represents the link status request message interaction information.

ls-update: represents the link status update message interaction information.

Recv: indicates information received.

Send: means sending the message.

Zebra: the debug information switch for the zebra process interaction.

【description】

debug ip ospf The command is used for open the relevant debugging information for the OSPF.

no debug ip ospf The command is used for close the relevant debugging information for the OSPF.

By default, all of the OSPF debugging switches are turned off.

debug ip ospf and **debug ospf** need to be opened at the same time before OSPF debugging will take effect.

【example】

#Open the event debug information switch for the OSPF.

Switch#configure terminal

Switch(config)#debug ip ospf event

Switch(config)#debug ospf

Chapter 33 Routing policy

33.1 Routing policy configuration command

33.1.1 ip access-list

【command】

Standard ACL:

ip access-list *standard-acl-number* **{ permit | deny }** *{ network wildcard-mask* **| any | host** *ip-address* **}**

no access-list *standard-acl-number* **[{ permit | deny }** *{ network wildcard-mask* **| any | host** *ip-address* **}]**

Extended ACL:

ip access-list *extended-acl-number* **{ permit | deny }** *{* **ip** *source-address wildcard-mask* **| any | host** *source-address* **}** *{ destination-address wildcard-mask* **| any | host** *destination-address* **}**

no access-list *extended-acl-number* **[{ permit | deny }** *{* **ip** *source-address wildcard-mask* **| any | host** *source-address* **}** *{ destination-address wildcard-mask* **| any | host** *destination-address* **}]**

Name ACL:

ip access-list *acl-name* **{ permit | deny }** *{ ip-prefix/length* **| any } [exact-match]**

no ip access-list *acl-name* **[{ permit | deny }** *{ ip-prefix/length* **| any } [exact-match]]**

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

standard-acl-number: Standard ACL number, value range 1-99 and 1300-1999.

permit: Specifies that the matching pattern of the ACL list is allowed.

deny: Specifies that the matching pattern for the ACL list is prohibited.

network wildcard-mask: Target network segment and reverse mask.

any: Represents the address of all the network segments.

host *ip-address*: Host address, indicating that the reverse mask address is 0.0.0.0.

extended-acl-number: Extend ACL number with values range 100-199 and 2000-2699.

source-address wildcard-mask : Wildcards for target segment addresses and target segment addresses.

host *source-address*: The address of the target network segment, and the wildcard character is 0.0.0.0.

destination-address wildcard-mask: wildcards for the masked and masked addresses.

host *destination-address*: Mask the address, and the wildcard character is 0.0.0.0.

acl-name: ACL name, for the 1-32 length string.

ip-prefix/length: Address prefix and mask length.

exact-match: Indicates that the prefix matches perfectly.

【description】

ip access-list The command is used for Configure the ACL filtering rule.

no ip access-list The command is used for Remove the ACL filtering rule.

By default, the ACL filter rule is not configured.

An ACL list can contain multiple table items, and the relationship between each table item is "or". In the process of matching, the device is checked according to the configuration of the table item. As long as the upper table item is matched, it means that the filtering of the ACL list is passed, and the next table item is not checked.

ACL list finally, contains implicit banned all table items: deny any, when certain routes are banned by configuring the deny statement, it is recommended to add a permit any statement at the end to allow other routes to pass.

【example】

#Configuring ACL filtering rule 1: refuse to learn 1.1.1.0/24 routes, can learn other routes.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip access-list 1 deny 1.1.1.0 0.0.0.255

Switch(config-router-rip)#ip access-list 1 permit any

#Configure to apply filtering rule 1 in RIP.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#distribute-list 1 in

33.1.2 ip prefix-list

【command】

ip prefix-list *prefix-name* **[seq** *seq-value*] **{ permit | deny } {** *network/length* **[ge** *ge-value* **] [le** *le-value* **] | any }**

no ip prefix-list *prefix-name* **[[seq** *seq-value*] **{ permit | deny } {** *network/length* **[ge** *ge-value* **] [le** *le-value* **] | any }]**

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

prefix-name: Prefix list name, values range from 1-32 characters.

seq *seq-value*: Specify the serial number of this rule in this prefix list, preferentially matching the table items with small check numbers in the range of 1-2147483647. By default, the serial number starts at 5 and increases in length by 5.

permit: Specifies that the matching pattern for the prefix list is allowed.

deny: Specifies that the matching pattern of the prefix list is prohibited.

network/length: Address prefix and mask length.

ge *ge-value*: The ge representation is greater than or equal to. Configure the minimum prefix length used for matching, with values ranging from length <ge-value <= le-value <=32.

le *le-value*: The le representation is less than or equal to. Configure the maximum prefix length used for matching, with values ranging from length <ge-value <= le-value <=32。

any: Represents the address of all the network segments.

【description】

ip prefix-list The command is used for Configure the IPv4 prefix list.

no ip prefix-list The command is used for Remove the specified IPv4 prefix list.

By default, the IPv4 prefix list is not configured.

An IPv4 prefix list can contain multiple table items, and the relationship between each table item is "or". In the process of matching, the device will check in ascending order according to the serial number corresponding to the table item. As long as a table item is matched, it means that through the filtering of the prefix list, and the next table item will not be checked.

Notes:

IPv4 prefix address range can be determined by length with [ge-value, The le-value] was determined that, When the gege-value and lele-value are not specified, The prefix mask length is the length; When only gege-value, The prefix mask length ranges from [ge-value, 32]; When only the lele-value is specified, The prefix mask length range is [length, le-value]; When both are specified, The prefix mask length ranges from [le-value, ge-value].

Finally, with implicitly all prohibited table items: deny any. When certain routes are banned by configuring the deny statement, it is recommended to add a permit any statement at the end to allow other routes to pass.

【example】

Configure a prefix list named aa: allow 1.0.0.0/8 segments with mask length ranging from 16 (16) to 24 (24).Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip prefix-list aa permit 1.0.0.0/8 ge 16 le 24

#Configure the application prefix list aa in RIP.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#distribute-list prefix aa in

33.1.3 ip prefix-list sequence-number

【command】

ip prefix-list sequence-number

no ip prefix-list sequence-number

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

None

【description】

ip prefix-list sequence-number The command is used for Enables the table item number in the prefix list.

no ip prefix-list sequence-number The command is used for Unshow the table item serial number in the prefix list。

By default, the serial number of each table item is displayed in the prefix list.

【example】

#The serial number is not displayed in the configuration prefix list.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#no ip prefix-list sequence-number

33.1.4 ipv6 access-list

【command】

ipv6 access-list *acl-name* **{ permit | deny } {** *prefix/length* **| any }**

no ipv6 access-list *acl-name* **[{ permit | deny } {** *prefix/length* **| any }]**

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

acl-name: Access control list name, the value range is 1 to 32 characters.

permit: Represents that the matching pattern of the specified ACL list is allowed.

deny: Represents that the matching pattern of the specified ACL list is prohibited.

prefix/length: The IPV 6 prefix and the mask length.

any: All network segments.

【description】

ipv6 access-list The command is used for Configure the ACL filtering rule.

no ipv6 access-list The command is used for Remove the ACL filtering rule.

By default, the ACL filter rule is not configured.

An ACL list can contain multiple table items, and the relationship between each table item is "or". In the process of matching, the device is checked according to the configuration of the table item. As long as the upper table item is matched, it means that the filtering of the ACL list is passed, and the next table item is not checked

The ACL list finally contains implicitly banned all table items: deny any. When certain routes are banned by configuring the deny statement, it is recommended to add a permit any statement at the end to allow other routes to pass.

【example】

#Configure ACL list named aa: only 2000:: / 64 network segment routing is allowed.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#ipv6 access-list aa permit 2000::/64

#Configure the Apply ACL list aa in RIPNG.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#distribute-list aa in

33.1.5 ipv6 prefix-list

【command】

ipv6 prefix-list *prefix-name* **[seq** *seq-value*] **{ permit | deny } {** *network/length* **[ge** *ge-value* **] [le** *le-value* **] | any }**

no ipv6 prefix-list *prefix-name* **[[seq** *seq-value*] **{ permit | deny } {** *network/length* **[ge** *ge-value* **] [le** *le-value* **] | any }]**

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

prefix-name: Prefix list name, value range from 1 to 32 characters.

seq-value: Specify the serial number of this rule in this prefix list, and preferentially match the small table items, which range from 1 to 2147483647. By default, the serial number starts at 5 and increases in length by 5.

permit: Specifies that the matching pattern for the prefix list is allowed.

deny: Specifies that the matching pattern of the prefix list is prohibited.

network/length: The IPV 6 address prefix and the mask length.

ge *ge-value*: The ge representation is greater than or equal to. Configure the minimum prefix length used for matching, with values ranging from length <ge-value <= le-value <=32.

le *le-value*: The le representation is less than or equal to. Configure the maximum prefix length used for matching, with values ranging from length <ge-value <= le-value <=32.

any: Represents the address of all the network segments.

【description】

ipv6 prefix-list The command is used for Configure the IPv6 prefix list.

no ipv6 prefix-list The command is used for Remove the IPv6 prefix list.

By default, the IPv6 prefix list is not configured.

An IPv6 prefix list can contain multiple table items, and the relationship between each table item is "or". In the process of matching, the device will check in ascending order according to the serial number corresponding to the table item. As long as a table item is matched, it means that through the filtering of the prefix list, and the next table item will not be checked.

Notes:

The ipv 6 prefix address range can be determined by length with [ge-value, The le-value] is determined that, When the gege-value and lele-value are not specified, The prefix mask length is the length; When only gege-value, The prefix mask length ranges from [ge-value, 128]; When only the lele-value is specified, The prefix mask length range is [length, le-value]; When both are specified, The prefix mask length ranges from [le-value, ge-value].

Finally, with implicitly all prohibited table items: deny any. When certain routes are banned by configuring a deny statement, it is recommended to add a permit any statement at the end to allow other routes to pass.

【example】

#Configure a prefix list named aa: 2000:: / 32 with a lengths between 64 (64) and 96 (96).

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#ipv6 prefix-list aa permit 2000::/32 ge 64 le 96

#Configure the application prefix list aa in RIPNG.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#distribute-list prefix aa in

33.1.6 ipv6 prefix-list sequence-number

【command】

ipv6 prefix-list sequence-number

no ip prefix-list sequence-number

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

None

【description】

ip prefix-list sequence-number The command is used for Enables the table item number in the prefix list.

no ipv6 prefix-list sequence-number The command is used for Unshow the table item serial number in the prefix list.

By default, the serial number of each table item is displayed in the enabling prefix list.

【example】

#The unprefix list displays the serial number.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#no ipv6 prefix-list sequence-number

33.1.7 route-map

【command】

route-map *route-map-name* { **permit** | **deny** } *seq-number*

no route-map *route-map-name* **[{ permit | deny }** *seq-number* **]**

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

route-map-name: Routing map name, used to uniquely identify a routing map, up to 32 characters.

permit: Specifies that the matching pattern of the created route graph statement is allowed. Is allowed to pass when the routing item satisfies all match clauses of the statement and performs the set clause of the statement. If the routing item does not satisfy the match clause of the statement, check the next statement of the route graph.

deny: Specifies that the matching pattern of the created routing map statement is prohibited and is prohibited only if the routing item satisfies all match clauses of the statement. The set clause is not executed in the deny mode.

seq-number: The serial number is used to identify a statement in the routing map in the range of 1-65535. When the routing map is used for matching, it is checked in small to large order according to the serial number of the statement.

【description】

route-map The command is used for create a routing map and enter the routing map configuration mode.

no route-map The command is used for delete the specified route map.

The routing map is not configured by default.

A routing map is a tool that matches routing and sets routing attributes. A routing map consists of several statements, each statement consisting of some match clause and set clauses. The match clause defines the matching rule for the statement, and the set clause defines the action after matching through the match clause. The relationship between match clauses is the relationship "with", that is, all match clauses of the statement must meet the requirements.

The relationship between routing map statements is "or". During the matching process, the device checks the order according to the serial number of the statement. As long as the inspection of a statement, it means to match the routing map, and never checks the next statement. If no statement is passed, the routing map does not match.

Notes:

When the routing protocol applies the routing map, but the routing map is not configured, all objects fail to match.

When the match clause is not configured in the routing map, all the objects can match successfully.

When the ACL, prefix list associated with the match clause in the routing map does not exist, all objects fail to match.

【example】

#Configure a routing map named test, matching mode as allowed, and serial number as 1.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#

33.1.8 match interface

【command】

match interface { **supervlan-interface** | **vlan-interface** } *interface-id*

no match interface

【config-mode】

Route map configuration mode

【parameter】

interface-id: With the slogan, the configuration range depends on the interface type.

【description】

match interface The command is used for create a matching rule based on the outgoing interface.

no match interface The command is used for deletes the specified outgoing interface-based matching rule.

In default, there is no matching rule based on the outgoing interface in the routing map.

【example】

#A rule is defined in the routing map aa to match the routing information of the interface as the interface vlan 50

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#match interface vlan-interface 50

33.1.9 match ip address

【command】

match ip address { *access-list-number* | *access-list-name* | **prefix-list** *prefix-name* }

no match ip address [prefix-list]

【config-mode】

Route map configuration mode

【parameter】

access-list-number: ACL ID.

access-list-name: ACL name.

prefix-name: ip prefix name.

【description】

match ip address The command is used for create a match rule based on the IP address information.

no match ip address The command is used for deletes the specified match rule based on the IP address information.

In default, there is no matching rule based on the IP address information in the routing map.

【example】

#A rule is defined in the routing map test to match the routing information of the IP address meeting the IP access control list 1.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip access-list 1 permit 1.1.1.0 0.0.0.255

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip address 1

33.1.10 match ip next-hop

【command】

match ip next-hop { *access-list-number* | *access-list-name* | **prefix-list** *prefix-name* }

no match ip next-hop [**prefix-list**]

【config-mode】

Route map configuration mode

【parameter】

access-list-number: Matches the ACL serial number.

access-list-name: Matching the ACL name.

prefix-name: Matching prefix list name.

【description】

match ip next-hop The command is used for create a match rule based on the routing of the next hop information.

no match ip next-hop The command is used for delete the specified match rule based on the routing next hop information.

In default, there is no matching rule based on the routing next jump information in the routing map.

【example】

#A rule is defined in the routing map test to match the routing information of the routing next hop address conforming to the IP access control list 1.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip access-list 1 permit 10.1.1.0 0.0.0.255

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip next-hop 1

33.1.11 match ip route-source

【command】

match ip route-source { *access-list-number* | *access-list-name* | **prefix-list** *prefix-name* }

no match ip route-source [prefix-list]

【config-mode】

Route map configuration mode

【parameter】

access-list-number: Matches the ACL serial number.

access-list-name: Matching the ACL name.

prefix-name: Matching prefix list name.

【description】

match ip route-source The command is used for create a matching rule based on the source address of the publication route.

no match ip route-source The command is used for delete the specified matching rule based on the source address based on the publication route.

By default, there is no matching rule based on the source address in the route graph.

【example】

#A rule is defined in the routing map test to match the routing information of the source address of the published route conforming to the IP Access Control List 1.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#ip access-list 1 permit 10.1.1.0 0.0.0.255

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip route-source 1

33.1.12 match metric

【command】

match metric *metric-value*

no match metric

【config-mode】

Route map configuration mode

【parameter】

metric-value: Matched routing overhead, with a range of 0-4294967295.

【description】

match metric The command is used for create a matching rule based on the routing overhead.

no match metric The command is used for remove matching rules based on routing overhead.

By default, there are no matching rules based on the routing overhead in the routing map.

【example】

#A rule is defined in the routing map test that matches the routing information with a routing overhead value of 10.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#match metric 10

33.1.13 match tag

【command】

match tag *tag-value*

no match tag

【config-mode】

Route map configuration mode

【parameter】

tag-value: Routing information marks values, range 0-65535.

【description】

match tag The command is used for create a match rule based on the routing information tag (Tag).

no match tag The command is used for remove the matching rule based on the Tag.

In default, there are no Tag-based matching rules in the routing policy.

【example】

#Define a rule in the routing map test to match the routing information with the marker field 8.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#match tag 10

33.1.14 match as-path

【command】

match as-path *as-path-name*

no match as-path

【config-mode】

Route map configuration mode

【parameter】

as-path-name: Matching AS-PATH list serial number, ranging from 1 to 199.

【description】

match as-path The command is used for create a matching rule based on the AS path filter.

no match as-path The command is used for remove the specified match rule based on the AS path filter.

By default, there is no matching rule based on the AS path filter in the routing policy.

According to the AS-PATH attribute of routing information, specify matching conditions to filter BGP routing information.

Configuration-reference command **ip as-path** for the AS-PATH list.

【example】

#Set the AS path filter with serial number 1 to allow the AS100 in the routing information. Then define a Route-map named test and define a match rule that refers to the AS path filter.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#ip as-path access-list 1 permit 100

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match as-path 1

33.1.15 match origin

【command】

match origin { egp | igp | incomplete }

no match origin

【config-mode】

Route map configuration mode

【parameter】

egp: Represents that the Origin property of BGP routing is egp.

igp: Represents that the Origin property of BGP routing is igp.

incomplete: Indicates that the Origin attribute of the BGP route is another route.

【description】

match origin The command is used for create a matching rule based on the origin of the BGP routing.

no match origin The command is used for remove the matching rules based on the origin of the BGP routing.

By default, there are no matching rules based on the BGP routing origin in the routing map.

【example】

#Rules are defined in the routing map of the test and are used to match the routing information where the BGP routing source is igp.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match origin igp

33.1.16 match probability

【command】

match probability *percentage*

no match probability

【config-mode】

Route map configuration mode

【parameter】

percentage: Percentage of the total number of routes.

【description】

match probability The command is used for create a match rule based on the percentage of the total number of routes.

no match probability The command is used for delete a matching rule based on the percentage of the total number of routes.

By default, there is no matching rule based on the percentage of the total number of routes in the routing map.

【example】

#Rules are defined in the routing map of the test and are used to match 50% of the routing information.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match probability 50

33.1.17 set ip next-hop

【command】

set ip next-hop *ip-address*

no set ip next-hop

【config-mode】

Route map configuration mode

【parameter】

ip-address: The next hop address of the route, points in a decimal format.

【description】

set ip next-hop The command is used for configure the action to change the next hop address of the route.

no set ip next-hop The command is used for restore the default situation.

By default, the action to change the next hop routing address is not configured in the routing map.

【example】

#Configure the routing map test: set the next hop address of the routing 1.1.1.0/24 to 10.1.1.1.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#ip access-list 1 permit 1.1.1.0 0.0.0.255

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip address 1

Switch(config-router-routemap-test-1)#set ip next-hop 10.1.1.1

33.1.18 set metric

【command】

set metric *{ metric | +metric | -metric }*

no set metric

【config-mode】

Route map configuration mode

【parameter】

metric: Routing overhead value, the value range 0~4294967295, the smaller the more preferred.

+metric: Increased routing overhead value.

-metric: Reduced routing overhead values.

【description】

set metric The command is used for configure actions to change the overhead value of the routing in the routing map.

no set metric The command is used for restore the default configuration.

By default, actions to change the overhead value of the routing are not configured in the routing map.

【example】

#Define access-list list with serial number 1, allowing the routing of 1.1.1.0/24 network segment to pass.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#ip access-list 1 permit 1.1.1.0 0.0.0.255

#Deine a routing map named test with serial number 1 and sets the overhead value for matching the routing to access-list list 1 to 20.

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip address 1

Switch(config-router-routemap-test-1)#set metric 20

33.1.19 set metric-type

【command】

set metric-type { type-1 | type-2 }

no set metric-type

【config-mode】

Route map configuration mode

【parameter】

type-1: The OSPF Class I external route.

type-2: OSPF Class II external routing.

【description】

set metric-type The command is used for configure actions to change the overhead type of the routing in the routing map.

no set metric-type The command is used for restore the default configuration.

By default, actions that change the overhead type of the routing are not configured in the routing map.

【example】

#Deine a routing map named aa, setting the type of routing overhead as type-1.

Switch#configure terminal

Switch(config)#router ospf

Switch(config-router-ospf)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#set metric-type type-1

#Apply routing map when republishing routing.

Switch(config-router-ospf)#redistribute rip route-map aa

33.1.20 set tag

【command】

set tag *tag-value*

no set tag

【config-mode】

Route map configuration mode

【parameter】

tag-value: Route tag value, value range 0-65535.

【description】

set tag The command is used for the action to change the routing information tag (Tag) is configured in the routing map.

no set tag The command is used for Restore the default configuration.

By default, the action to change the routing information tag (Tag) is not configured in the routing map.

【example】

#Set the tag (Tag) value for the routing information to 10.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#set tag 10

33.1.21 set local-preference

【command】

set local-preference *value*

no set local-preference

【config-mode】

Route map configuration mode

【parameter】

value: BGP routes local priority and values range from 0 to 4294967295. A larger value indicates a higher priority.

【description】

set local-preference The command is used for the action to change the local priority of the BGP routing information is configured in the routing map.

no set local-preference The command is used for restore the default configuration.

By default, actions that change the local priority of the BGP routing information are not configured in the routing map.

【example】

#Define access-list list with serial number 1, allowing the routing of 1.1.1.0/24 network segment to pass.

#Set the local priority of the BGP routing information to 200.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#ip access-list 1 permit 1.1.1.0 0.0.0.255

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip address 1

Switch(config-router-routemap-test-1)#set local-preference 200

33.1.22 set origin

【command】

set origin { egp | igp | incomplete }

no set origin

【config-mode】

Route map configuration mode

【parameter】

egp: Indicates that the BGP routing information source is specified as an external route.

igp: Indicates the BGP routing information source as internal routing.

incomplete: Represents that the specified BGP routing information source is unknown.

【description】

set origin The command is used for the action to change the Origin property of BGP routing in the routing map.

no set origin The command is used for restore the default configuration.

By default, the action to change the Origin attribute of the BGP routing is not configured in the routing map.

【example】

#Set the route source of the route 1.1.1.0/24 to be the egp.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#ip access-list 1 permit 1.1.1.0 0.0.0.255

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip address 1

Switch(config-router-routemap-test-1)#set origin egp

33.1.23 set weight

【command】

set weight *weight-value*

no set weight

【config-mode】

Route map configuration mode

【parameter】

weight-value: Weight value of BGP routing, taking the value range from 0 to 4294967295.

【description】

set weight The command is used for action action to change the weight of BGP routing in the routing map.

no set weight The command is used for restore default configuration.

In default, the action to change the weight of the BGP routing is not configured in the routing map.

【example】

#Set the weight of the BGP routing 1.1.1.0/24 to 200.

Switch#configure terminal

Switch(config)#router bgp 100

Switch(config-router-bgp)#ip access-list 1 permit 1.1.1.0 0.0.0.255

Switch(config-router-bgp)#route-map test permit 1

Switch(config-router-routemap-test-1)#match ip address 1

Switch(config-router-routemap-test-1)#set weight 200

33.1.24 call

【command】

call *route-map-name*

no call

【config-mode】

Route map configuration mode

【parameter】

route-map-name: route map name.

【description】

call The command is used for set up to jump to another route map match.

no call The command is used for restore the default configuration.

In default, the routing map jump is not configured, that is, after the routing map matches through the current routing map, no other graphs are matched.

【example】

#Deine a routing map named aa and sets the metric value of the routing to 20.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#set metric 20

#Define a routing map named test, serial number 1, jump to the routing map aa for matching.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#call aa

33.1.25 continue

【command】

continue [*seq-number*]

no continue

【config-mode】

Route map configuration mode

【parameter】

seq-number: The execution node number of this routing map, and the value range is 1-65535.

【description】

continue The command is used for configure the next execution node.

no continue The command is used for restore the default configuration.

In default, the next execution node is not configured, that is, after the current node match, the other node matches are not matched.

The next execution node, the serial number must be larger than the current node serial number.

【example】

#Define a routing map named test, with the serial number as 1, and configure the next execution node as 5.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#continue 5

33.1.26 on-match

【command】

on-match { goto *seq-number* **| next }**

no on-match { goto | next }

【config-mode】

Route map configuration mode

【parameter】

goto *seq-number*: The execution node number of this routing map, and the value range is 1-65535.

next: The next execution node.

【description】

on-match The command is used for configure the next execution node.

no on-match The command is used for restore the default situation.

By default, the next execution node is not configured.

The next execution node, the serial number must be larger than the current node serial number.

【example】

#Define a routing map named test, with the serial number as 1, and configure the next execution node as 5.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map test permit 1

Switch(config-router-routemap-test-1)#on-match goto 5

33.1.27 route-map in

【command】

route-map *route-map-name* **in { supervlan-interface | vlan-interface }** *interface-id*

no route-map *route-map-name* **in { supervlan-interface | vlan-interface }** *interface-id*

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

route-map-name: Route graph name, a maximum length of 32 characters.

in: Indicates the direction.

interface-id: Interface ID, the configuration range depends on the interface type.

【description】

route-map in The command is used for the route map is applied when the configuration interface learns the routing.

no route-map in The command is used for restore the default situation.

By default, the route map is not applied.

To create the route map before applying the route map, refer to the command: **route-map**.

【example】

#Configuration to apply routing maps when the vlan 50 interface learns routing.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#match metric 10

Switch(config-router-routemap-aa-1)#set metric 2

Switch(config-router-rip)#route-map aa in vlan-interface 50

33.1.28 route-map out

【command】

route-map *route-map-name* **out { supervlan-interface | vlan-interface }** *interface-id*

no route-map *route-map-name* **out { supervlan-interface | vlan-interface }** *interface-id*

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

route-map-name: route map name.

out: Indicate the direction, that is, matching the route graph when publishing the route.

interface-id: Interface ID, the configuration range depends on the interface type.

【description】

route-map out The command is used for configure the interface when publishing the route.

no route-map out The command is used for Restore the default situation.

By default, the route map is not applied.

To create the route map before applying the route map, refer to the command: **route-map**.

【example】

#Configure to apply the routing map when the vlan 50 interface publishes the routing.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#route-map aa permit 1

Switch(config-router-routemap-aa-1)#match metric 10

Switch(config-router-routemap-aa-1)#match metric 5

Switch(config-router-rip)#route-map aa out vlan-interface 50

33.2 Routing policy monitoring and debugging command

33.2.1 show route-map

【command】

show route-map [*route-map-name*]

【config-mode】

RIP/RIPng/OSPF/OSPFv3/BGP configuration mode

【parameter】

route-map-name: route map name , for uniquely identifying a routing map, up to 32 characters.

【description】

show route-map The command is used for displays the routing map information.

【example】

#View the routing map information.

dut1(config-router-rip)#show route-map

route-map aa, permit, sequence 1

Call clause:

Action:

Exit routemap

Match clauses:

origin igp

Set clauses:

metric 300

show route-map field description

Field	Description
route-map	Route map name
permit	Matching pattern of the routing map statement, permit for allowed and deny for prohibited
sequence	sequence
Call clause	Jump to another routing map

Action	By default, the exit route map is completed, and modification is not supported
Match clauses	Match clauses
Set clauses	Set clauses

33.2.2 clear ip prefix-list

【command】

clear ip prefix-list [***prefix-name*** **]**

【config-mode】

RIP/OSPF/BGP configuration mode

【parameter】

prefix-name: Prefix list name, values range from 1-32 characters.

【description】

clear ip prefix-list The command is used for clear the prefix list statistics.

【example】

#Clear the prefix list statistics.

Switch#configure terminal

Switch(config)#router rip

Switch(config-router-rip)#clear ip prefix-list

33.2.3 clear ipv6 prefix-list

【command】

clear ipv6 prefix-list [*prefix-name* **]**

【config-mode】

OSPFv3/RIPng configuration mode

【parameter】

prefix-name: Prefix list name, value range from 1 to 32 characters.

【description】

clear ipv6 prefix-list The command is used for clear the prefix list statistics.

【example】

#Clear the prefix list statistics.

Switch#configure terminal

Switch(config)#router ripng

Switch(config-router-ripng)#clear ipv6 prefix-list

33.2.4 show ip access-list

【command】

show ip access-list [*access-list-number* | *access-list-name* **]**

【config-mode】

RIP/OSPF/BGP configuration mode

【parameter】

access-list-number: ACL number.

access-list-name: ACL name.

【description】

show ip access-list The command is used for view the access control list information.

【example】

#View access-list list information.

Switch(config-router-rip)#show ip access-list

Standard IP access list 1: 2 entries

permit 1.1.1.0, wildcard bits 0.0.0.255

permit 1.1.2.0, wildcard bits 0.0.0.255

Extended IP access list 100: 1 entries

permit ip host 2.2.2.0 host 255.255.255.0

Zebra IP access list test: 1 entries

permit 3.3.3.0/24

Total entries: 3. Total rule entries: 4

show ip access-list field description

Field	Description
Standard IP access list	Standard ACL list information
Extended IP access	Extended IP access information
Zebra IP access list	Zebra IP access list information
Total entries	The total number of ACL is presented here
Total rule entries	The total number of rules available

33.2.5 show ip prefix-list

【command】

show ip prefix-list [detail | summary] [*prefix-name*]

【config-mode】

RIP/OSPF/BGP configuration mode

【parameter】

prefix-name: Name of the prefix list, the value range 1-32 characters.

detail: Indicates the details of the display prefix list.

summary: Indicates the summary information that displays the prefix list.

【description】

show ip prefix-list The command is used for view the prefix list information.

【example】

#View the details of the prefix list.

Switch(config-router-rip)#show ip prefix-list detail

ip prefix-list 1:

Description:

count: 1, range entries: 0, sequences: 5 - 5

seq 5 deny 1.1.1.0/24 (hit count: 2, refcount: 20)

Total entries: 1. Total rule entries: 1

show ip prefix-list detail field description

Field	Description
ip prefix-list	Prefix list name
count	Number of the prefix list statements
range entries	Number of routes that meet the matching criteria, and the display of this field is currently not supported

Sequences	Range of the prefix list sequences number
hit count	Number of routes that qualify for the table item
refcount	Reference count

33.2.6 show ipv6 access-list

【command】

show ipv6 access-list [*acl-name* **]**

【config-mode】

OSPFv3/RIPng configuration mode

【parameter】

acl-name: Access control list name, the value range is 1 to 32 characters.

【description】

show ipv6 access-list The command is used for view the access control list information.

【example】

#View access-list list information.

Switch(config-router-ripng)#show ipv6 access-list

Zebra IPv6 access list 1: 1 entries

permit 2000::/64

Total entries: 1. Total rule entries: 1

show ipv6 access-list field description

Field	Description
Zebra IPv6 access list	The ACL name list information
Total entries	The total number of ACL is presented here
Total rule entries	The total number of rules available

33.2.7 s show ipv6 prefix-list

【command】

show ipv6 prefix-list [detail | summary] [*prefix-name* **]**

show ipv6 prefix-list *prefix-name* **[seq** *seq-number* | *network/length* **[first-match | longer]]**

【config-mode】

OSPFv3/RIPng configuration mode

【parameter】

detail: Indicates the details of the display prefix list.

summary: Indicates the summary information that displays the prefix list.

prefix-name: Prefix list name, value range from 1 to 32 characters.

seq-number: Sequences number, and the values range from 1 to 65535.

network/length: Address prefix and mask length.

first-match: Represents the item showing the first match.

longer: Represents the item showing the longest match.

【description】

show ipv6 prefix-list The command is used for view the prefix list information.

【example】

#View the details of the prefix list.

Switch(config-router-ripng)#show ipv6 prefix-list detail

ipv6 prefix-list aa:

Description:

count: 1, range entries: 0, sequences: 5 - 5

seq 5 permit 3000::/64 (hit count: 0, refcount: 0)

Total entries: 1. Total rule entries: 1

show ipv6 prefix-list detail field description

Field	Description
ipv6 prefix-list	Prefix list name
count	Number of the prefix list statements
range entries	Number of routes that meet the matching criteria. Display of this field is not supported
Sequences	Range of the prefix list serial number
hit count	Number of routes that qualify for the table item
refcount	reference count

Chapter 34 L2 Multicast Basic

34.1 L2 Multicast basic config command

34.1.1 unknown-discard multicast vlan

【command】

unknown-discard multicast vlan *vlan-list*

no unknown-discard multicast vlan *vlan-list*

【config-mode】

global config-mode

【parameter】

vlan-list: VLAN list value, 1-128 length string format, e.g., 1-3,5.

【description】

unknown-discard multicast vlan command is used to enable unknown multicast discarding.

no unknown-discard multicast vlan command is used to disable unknown multicast discarding.

By default, unknown multicast discarding is disabled, that means flooding all unknown multicast in any VLAN.

【example】

#enable unknown multicast discarding in VLAN 1-2.

Switch#configure terminal

Switch(config)#no unknown-discard multicast vlan 1,2

34.1.2 multicast mac-address vlan

【command】

multicast mac-address *mac-address* **vlan** *vlan-id*

no multicast mac-address *mac-address* **vlan** *vlan-id*

【config-mode】

global config-mode

【parameter】

mac-address: MAC address, colon-hexadecimal format, e.g., 01:00:5e:H:H:H.

vlan-id: VLAN ID value, value range is 1-4094.

【description】

multicast mac-address vlan command is used to config l2 static multicast entry.

no multicast mac-address command is used to unconfig l2 static multicast entry.

By default, none of static multicast entry is configured.

Instruction:

⇌ The MAC address configured must be a legal multicast MAC address and cannot be broadcast or unicast.

【example】

#config static multicast entry 01:00:5e:0:00:01 vlan 1.

Switch#configure terminal

Switch(config)#multicast mac-address 01:00:5e:00:00:01 vlan 1

34.1.3 multicast mac-address vlan interface

【command】

multicast mac-address *mac-address* **vlan** *vlan-id* **interface { all | ethernet** *port-id* **}**

no multicast mac-address *mac-address* **vlan** *vlan-id* **interface { all | ethernet** *port-id* **}**

【config-mode】

global config-mode

【parameter】

mac-address: MAC address, colon-hexadecimal format, e.g., 01:00:5e:H:H:H.

vlan-id: VLAN ID value, value range is 1-4094.

all: all ports.

port-id: Port ID value, stack-id/slot-id/port-id format, e.g., 0/0/1.

【description】

multicast mac-address vlan interface command is used to add l2 static multicast entry member port.

no multicast mac-address vlan interface command is used to delete l2 static multicast entry member port.

By default, none of port is added to any of multicast entry.

【example】

#add port ethernet 0/0/1 to static multicast entry 01:00:5e:0:00:01 VLAN 1

Switch#configure terminal

Switch(config)#multicast mac-address 01:00:5e:00:00:01 vlan 1

Switch(config)#multicast mac-address 01:00:5e:00:00:01 vlan 1 interface ethernet 0/0/1

34.2 L2 Multicast Basic Monitor and Debug

34.2.1 show unknown-discard vlan

【command】

show unknown-discard vlan [*vlan-id*]

【config-mode】

any

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

【description】

show unknown-discard vlan command is used to display unknown multicast discarding configuration.

【example】

#display unknown multicast discarding configuration in all VLAN.

Switch#configure terminal

Switch(config)#show unknown-discard vlan

unknown multicast vlan list : 1-2

34.2.2 show multicast

【command】

show multicast [**mac-address** *mac-address* [**vlan** *vlan-id* [**interface** { **all** | **ethernet** *port-id* }]]]

【config-mode】

any

【parameter】

mac-address: MAC address, support IPv4 and IPv6 MAC format, e.g., 01:00:5e:H:H:H/33:33:H:H:H:H.

vlan-id: VLAN ID value, value range is 1-4094.

all: all ports.

port-id: Port ID value, stack-id/slot-id/port-id format, e.g., 0/0/1.

【description】

show multicast command is used to display all or group-specific multicast forwarding entry.

【example】

#display all multicast forwarding entry

Switch(config)#show multicast

show multicast table information

MAC Address : 01:00:5e:00:00:01

VLAN ID : 1

Static port list : e0/0/1.

IGMP port list : e0/0/7.

Dynamic port list :

Total entries: 1.

show multicast filed description

Filed	Description
MAC Address	l2 multicast MAC address
VLAN ID	VLAN of l2 multicast
Static port list	static member port list
IGMP port list	IGMP snooping member port list
Dynamic port list	GMRP member port list

34.2.3 debug multicast

【command】

debug multicast

no debug multicast

【config-mode】

global config-mode

【parameter】

none

【description】

debug multicast command is used to enable multicast debug.

no debug multicast command is used to disable multicast debug.

By default, l2 multicast debug is disabled.

【example】

#enable multicast debug

Switch#configure terminal

Switch(config)#debug multicast

Chapter 35 IGMP-snooping

35.1 IGMP-snooping config command

35.1.1 igmp-snooping

【command】

igmp-snooping

no igmp-snooping

【config-mode】

global config-mode

【parameter】

none

【description】

igmp-snooping command is used to enable IGMP Snooping.

no igmp-snooping command is used to disable IGMP Snooping.

By default, global IGMP Snooping is disabled.

【example】

#enable global IGMP snooping

Switch#configure terminal

Switch(config)#igmp-snooping

35.1.2 igmp-snooping enable-vlan

【command】

igmp-snooping enable-vlan *vlan-id*

no igmp-snooping enable-vlan *vlan-id*

【config-mode】

global config-mode

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

【description】

igmp-snooping enable-vlan command is used to enable specific VLAN IGMP snooping.

no igmp-snooping enable-vlan command is used to disable specific VLAN IGMP snooping

By default, all VLAN IGMP snooping is disabled.

【example】

#enable VLAN 1 IGMP snooping

Switch#configure terminal

Switch(config)#igmp-snooping enable-vlan 1

35.1.3 igmp-snooping version

【command】

igmp-snooping version *version-value*

【config-mode】

global config-mode

【parameter】

version-value: protocol version number, value range is 2-3, default is 2.

【description】

igmp-snooping version command is used to config version.

【example】

#config IGMP snooping version to 3

Switch#configure terminal

Switch(config)#igmp-snooping version 3

35.1.4 igmp-snooping host-aging-time

【command】

igmp-snooping host-aging-time *time-value* **[vlan** *vlan-id* **]**

no igmp-snooping host-aging-time *host-aging-time-value* **[vlan** *vlan-id* **]**

【config-mode】

global config-mode

【parameter】

time-value: member port expired time, value range is 0-1000000 in second.

vlan-id: VLAN ID value, value range is 1-4094.

【description】

igmp-snooping host-aging-time command is used to config multicast member static expired time

no igmp-snooping host-aging-time command is used to return to the default situation.

By default, static expired time is not configured.Multicast member dynamic expired time = robust-count * query-interval + max-response-time.

After configuring static expired time, the dynamic expired time is ineffective.

【example】

#config VLAN 1 host-aging-time to 300 seconds.

Switch#configure terminal

Switch(config)#igmp-snooping host-aging-time 300 vlan 1

35.1.5 igmp-snooping max-response-time

【command】

igmp-snooping max-response-time *time-value*

no igmp-snooping max-response-time

【config-mode】

global config-mode

【parameter】

time-value: general query max response time value, value range is 1-100 in second,default is 10.

【description】

igmp-snooping max-response-time command is used to config general query max response time.

no igmp-snooping max-response-time command is used to return to default .

By default, general query max response time is 10 second.

【example】

#config general query max response time to 15 seconds.

Switch#configure terminal

Switch(config)#igmp-snooping max-response-time 15

35.1.6 igmp-snooping robust-count

【command】

igmp-snooping robust-count *robust-count-value*

no igmp-snooping robust-count

【config-mode】

global config-mode

【parameter】

robust-count-value: group-specific query robust count, value range is 1-5, default is 2.

【description】

igmp-snooping robust-count command is used to config group-specific query robust count.

no igmp-snooping robust-count command is used to return to default.

By default, when Querier receives leave message, it will send group-specific query twice.

【example】

#config group-specifc query robust count to 3.

Switch#configure terminal

Switch(config)#igmp-snooping robust-count 3

35.1.7 igmp-snooping last-member-query-interval

【command】

igmp-snooping last-member-query-interval *query-interval-value*

no igmp-snooping last-member-query-interval

【config-mode】

global config-mode

【parameter】

query-interval-value: Group-specific query period time value in the range 1-5 in seconds, default value is 1.

【description】

igmp-snooping last-member-query-interval The command is used to configure the query interval for a specific group.

no igmp-snooping last-member-query-interval command is used to return to default.

The query interval is effective when the number of times a group-specific query message is sent is greater than 1.

【example】

#Configure the sending interval for group-specific query messages to 3 seconds.

Switch#configure terminal

Switch(config)#igmp-snooping last-member-query-interval 3

35.1.8 igmp-snooping fast-leave

【command】

igmp-snooping fast-leave

no igmp-snooping fast-leave

【config-mode】

Port configuration mode

【parameter】

none

【description】

igmp-snooping fast-leave command to enable the Quick Leave function.

no igmp-snooping fast-leave command to disable the Quick Leave function.

By default, the fast leave function is disabled.

Close fast-leave when a leave message is received, aging members according to aging time；

When fast leave is enabled, multicast table entries are deleted immediately when a leave message is received.

【example】

#Enable fast leave function for port ethernet 0/0/1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#igmp-snooping fast-leave

35.1.9 igmp-snooping group-limit

【command】

igmp-snooping group-limit *limit-value*

no igmp-snooping group-limit

【config-mode】

port configuration mode

【parameter】

limit-value: Multicast limit value, from 0 to 1024, default value is 1024.

【description】

igmp-snooping group-limit Command to configure the number of multicast groups a port can learn.

no igmp-snooping group-limit command is used to return to default.

When the number of multicasts learned by a port reaches the limit value, new join messages are discarded by default, i.e. no new multicast groups are learned.

【example】

#Configure the number of multicast groups that can be learned on port ethernet 0/0/1 to 10

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#igmp-snooping group-limit 10

35.1.10 igmp-snooping overflow-replace

【command】

igmp-snooping overflow-replace

no igmp-snooping overflow-replace

【config-mode】

global/port configuration mode

【parameter】

none

【description】

igmp-snooping overflow-replace command to enable the overflow replacement function.

no igmp-snooping overflow-replace command is used to return to default.

By default, the overflow replacement function is disabled.

After enabling the overflow-replace function, when the number of multicasts learned by a port reaches the limit value, the newly learned multicast group replaces the first learned multicast group.

After turning Off the overflow-replace function, when the number of multicast learned by the port reaches the limit value,

the join message will be discarded directly and no new multicast group will be learned.

【example】

#enable global overflow-replace function.

Switch#configure terminal

Switch(config)#igmp-snooping overflow-replace

35.1.11 igmp-snooping drop

【command】

igmp-snooping drop {query | report}

no igmp-snooping drop {query | report}

【config-mode】

port configuration mode

【parameter】

query: indicates an IGMP query message.

report: indicates an IGMP report message.

【description】

igmp-snooping drop the command enables the discard IGMP protocol packet function.

no igmp-snooping drop command to disable the discard IGMP protocol packets.

By default, discard is disabled.

【example】

#enable port ethernet 0/0/1 to discard IGMP query packets.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#igmp-snooping drop query

35.1.12 igmp-snooping multicast-vlan

【command】

igmp-snooping multicast-vlan *vlan-id*

no igmp-snooping multicast-vlan

【config-mode】

port configuration mode

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

【description】

igmp-snooping multicast-vlan command to enable port multicast VLAN function.

no igmp-snooping multicast-vlan command to disable port multicast VLAN function.

by default, the port is not enabled for multicast VLAN function.

when multicast VLAN is enabled, multicast-vlan will be used to learn multicast groups.

【example】

#enabling port ethernet 0/0/1 multicast VLAN to 100.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#igmp-snooping multicast-vlan 100

35.1.13 igmp-snooping static-group

【command】

igmp-snooping static-group *group-address* **[source-ip** *source-address* **] vlan** *vlan-id* **{ all | ethernet** *port-id* **}**

no igmp-snooping static-group *group-address* **[source-ip** *source-address* **] vlan** *vlan-id* **{ all | ethernet** *port-id* **}**

【config-mode】

global configuration mode

【parameter】

group-address: multicast group IP address value in dotted decimal, e.g. 225.0.0.1.

source-address: multicast source IP address value, in dotted decimal, e.g. 1.1.1.1.

vlan-id: VLAN ID value, value range is 1-4094.

port-id: port ID value, format stack number/slot number/port number, e.g. 0/0/1.

【description】

igmp-snooping static-group command to configure static multicast group table entries.

no igmp-snooping static-group command to delete a static multicast group table entry.

【example】

#configure a static multicast group: 225.0.0.1 VLAN 1 ethernet 0/0/1.

Switch#configure terminal

Switch(config)#igmp-snooping static-group 225.0.0.1 vlan 1 ethernet 0/0/1

35.1.14 igmp-snooping static-group proxy

【command】

igmp-snooping static-group proxy [interval *interval-value***]**

no igmp-snooping static-group proxy

【config-mode】

global configuration mode

【parameter】

interval-value: static multicast proxy period value in the range of 30-300 in seconds.

【description】

igmp-snooping static-group proxy command to enable the static multicast proxy function.

igmp-snooping static-group proxy interval command to configure multicast proxy intervals.

no igmp-snooping static-group proxy command to disable the static multicast proxy function.

By default, the static multicast proxy function is not enabled. If no multicast proxy cycle time is configured, the default is to proxy only once.

When the static multicast proxy feature is enabled, join messages will be sent to the multicast source (router port) periodically at interval-time intervals, or only once if no interval-time is configured.

【example】

#enabling IGMP snooping static multicast proxy function.

Switch#configure terminal

Switch(config)#igmp-snooping static-group proxy

35.1.15 igmp-snooping source-learning

【command】

igmp-snooping source-learning

no igmp-snooping source-learning

【config-mode】

global configuration mode

【parameter】

none

【description】

igmp-snooping source-learning command to enable learning multicast source function.

no igmp-snooping source-learning command to disable the learning multicast source function.

when running version 3, after enabling source-learning, IGMPv3 report will be received and multicast group will be learned and multicast source will be recorded; after disabling source-learning, IGMPv3 report message will be received and multicast group will be learned, but multicast source will not be recorded.

【example】

#enable source-learning function

Switch#configure terminal

Switch(config)#igmp-snooping source-learning

35.1.16 igmp-snooping querier

【command】

igmp-snooping querier

no igmp-snooping querier

【config-mode】

global configuration mode

【parameter】

none

【description】

igmp-snooping querier command is used to enable the querier function.

no igmp-snooping querier command to turn off the querier function.

By default, the querier function is not enabled.

【example】

#enabling the querier function.

Switch#configure terminal

Switch(config)#igmp-snooping querier

35.1.17 igmp-snooping querier-vlan

【command】

igmp-snooping querier-vlan *vlan-list-value*

no igmp-snooping querier-vlan [*vlan-list -value***]**

【config-mode】

global configuration mode

【parameter】

vlan-list-value: VLAN list value, formatted as a string of length 1-128, e.g. 1-3,5.

【description】

igmp-snooping querier-vlan command is used to enable the querier function of VLAN.

no igmp-snooping querier-vlan command to disable the querier function of VLAN.

By default, the query function of VLAN 1 is enabled.

The VLAN querier function will take effect only after the querier function is globally enabled.

【example】

#enable the querier function of VLAN 1,2.

Switch#configure terminal

Switch(config)#igmp-snooping querier-vlan 1,2

35.1.18 igmp-snooping querier-elect

【command】

igmp-snooping querier-elect

no igmp-snooping querier-elect

【config-mode】

global configuration mode

【parameter】

none

【description】

igmp-snooping querier-elect command to enable the querier election function.

no igmp-snooping querier-elect command to disable the querier election function.

By default, the querier election function is enabled.

If you turn off the query election function, you will not take part in the query election, i.e., you will be the queryer.

【example】

#enabling the querier election function.

Switch#configure terminal

Switch(config)#igmp-snooping querier-elect

35.1.19 igmp-snooping query-interval

【command】

igmp-snooping query-interval *query-interval-value*

no igmp-snooping query-interval

【config-mode】

global configuration mode

【parameter】

query-interval-value: common group query period value, the value range is 1-30000, unit of seconds, the default value 125.

【description】

igmp-snooping query-interval the command is used to configure the general group query interval.

no igmp-snooping query-interval command is used to return to default.

The query interval must be greater than the maximum response time.

【example】

#configure the query period time to 60s.

Switch#configure terminal

Switch(config)#igmp-snooping query-interval 60

35.1.20 igmp-snooping query-source

【command】

igmp-snooping query-source *ip-address*

no igmp-snooping query-source

【config-mode】

global configuration mode

【parameter】

ip-address: query the source IP address of the message, dotted decimal format, such as 1.1.1.1.

【description】

igmp-snooping query-source command is used to configure the source IP address of the query message.

no igmp-snooping query-source command is used to return to default.

by default, the IP address of the interface in the VLAN is used as the source IP address of the query message.

【example】

#configure the source IP address of the query message to 192.168.1.2.

Switch#configure terminal

Switch(config)#igmp-snooping query-source 192.168.1.2

35.1.21 igmp-snooping proxy

【command】

igmp-snooping proxy

no igmp-snooping proxy

【config-mode】

global configuration mode

【parameter】

none

【description】

igmp-snooping proxy command is used to enable the proxy function.

no igmp-snooping proxy command to disable the proxy function.

By default, the proxy function is disabled.

When the proxy function is enabled, a report message will be sent to the routing port only when a multicast forwarding table entry is created for the first time; a leave message will be sent to the routing port only when the last member of the multicast forwarding table leaves.

The source MAC and source IP of the proxy's report message are the MAC and VLAN interface IP of the proxy device.

The source MAC and source IP of the proxy's leave message are the MAC and VLAN interface IP of the proxy device.

【example】

#enabling query agent function.

Switch#configure terminal

Switch(config)#igmp-snooping query-proxy

35.1.22 igmp-snooping query-proxy

【command】

igmp-snooping query-proxy

no igmp-snooping query-proxy

【config-mode】

global configuration mode

【parameter】

none

【description】

igmp-snooping query-proxy command is used to enable the query agent function.

no igmp-snooping query-proxy command to disable the query agent function.

By default, the query agent function is enabled.

The query proxy will take effect only when the proxy function is enabled.

The source MAC and source IP of the proxy's query message are the MAC and VLAN interface IP of the proxy device.

【example】

#enabling query agent function.

Switch#configure terminal

Switch(config)#igmp-snooping query-proxy

35.1.23 igmp-snooping route-port

【command】

igmp-snooping route-port vlan *vlan-id* {**all | ethernet** *port-id*}

no igmp-snooping route-port [[vlan *vlan-id* **] [ethernet** *port-id* **]]***

【config-mode】

global configuration mode

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

port-id: port ID, format stacking number/slot number/port number, e.g., 0/0/1.

【description】

igmp-snooping route-port command is used to configure a static router port.

no igmp-snooping route-port command to delete static router port configuration.

【example】

#configure port ethernet 0/0/1 as a static router port inside VALN 1

Switch#configure terminal

Switch(config)#igmp-snooping router-port vlan 1 ethernet 0/0/1

35.1.24 igmp-snooping router-aging-time

【command】

igmp-snooping router-aging-time *aging-time-value*

no igmp-snooping router-aging-time

【config-mode】

global configuration mode

【parameter】

aging-time-value: router port aging time, the value range is 10-1000000, the unit of seconds, the default 300.

【description】

igmp-snooping router-aging-time command is used to configure the aging time of dynamic routing ports.

no igmp-snooping router-aging-time command is used to return to default.

By default, the router port aging time is 300 seconds.

【example】

#configure dynamic router port aging time to 200.

Switch#configure terminal

Switch(config)#igmp-snooping router-aging-time 200

35.1.25 igmp-snooping route-port forward

【command】

igmp-snooping route-port forward

no igmp-snooping route-port forward

【config-mode】

global configuration mode

【parameter】

none

【description】

igmp-snooping route-port forward the command enables the router port to forward multicast service packets.

no igmp-snooping route-port forward the command disables the router port forwarding function for multicast service messages.

By default, the router port forwarding function is not enabled.

After enabling the router port forwarding function, the router port is added as a member of IGMP Snooping multicast table entry, and thus can receive multicast packets.

When there is no IGMP Snooping multicast table entry, the router port will not forward multicast service messages even though the router port forwarding function is enabled.

【example】

#enable the router port forwarding function.

Switch#configure terminal

Switch(config)#igmp-snooping version route-port forward

35.1.26 igmp-snooping preview

【command】

igmp-snooping preview

no igmp-snooping preview

【config-mode】

gobal configuration mode

【parameter】

none

【description】

igmp-snooping preview the command enables the multicast preview function.

no igmp-snooping preview command to disable the multicast preview function.

By default, the multicast preview function is not enabled.

【example】

#enable multicast preview function.

Switch#configure terminal

Switch(config)#igmp-snooping preview

35.1.27 igmp-snooping preview group-ip

【command】

igmp-snooping preview group-ip *ip-address* **vlan** *vlan-id* **ethernet** *port-id*

no igmp-snooping preview group-ip *ip-address* **vlan** *vlan-id* **ethernet** *port-id*

【config-mode】

global configuration mode

【parameter】

ip-address: multicast group for multicast preview, dotted decimal, e.g., 225.0.0.1.

vlan-id: VLAN ID value, value range is 1-4094.

port-id: port ID in the format of stack number/slot number/port number, e.g., 0/0/1.

【description】

igmp-snooping preview group-ip the command is used to configure the preview multicast group.

no igmp-snooping preview group-ip command is used to delete the configuration.

By default, no preview multicast group exists.

【example】

#configure preview multicast group 225.0.0.2, VLAN 1, member ethernet 0/0/1.

Switch#configure terminal

Switch(config)#igmp-snooping preview group-ip 225.0.0.2 vlan 1 ethernet 0/0/1

35.1.28 igmp-snooping preview time-once

【command】

igmp-snooping preview time-once *time-once-value*

no igmp-snooping preview time-once

【config-mode】

global configuration mode

【parameter】

time-once-value: multicast preview working time value, the value range is 60-300, in seconds, the default value is 180.

【description】

igmp-snooping preview time-once command is used to configure the working time of each multicast preview.

no igmp-snooping preview time-once command is used to return to default.

The length of time the multicast group is in the online state, and the multicast messages can be forwarded in this state.

【example】

#configure the multicast preview function to last 60 seconds each time

Switch#configure terminal

Switch(config)#igmp-snooping preview time-once 60

35.1.29 igmp-snooping preview time-interval

【command】

igmp-snooping preview time-interval *time-interval-value*

no igmp-snooping preview time-interval

【config-mode】

global configuration mode

【parameter】

time-interval-value: multicast preview interval length, the value range is 180-600 in seconds, the default value is 300.

【description】

igmp-snooping preview time-interval the command is used to configure the multicast preview interval length.

no igmp-snooping time-interval command is used to return to default.

The length of time the multicast group is in the offline state, and multicast messages cannot be forwarded in this state.

【example】

#configure the multicast preview interval to 180 seconds

Switch#configure terminal

Switch(config)#igmp-snooping preview time-interval 180

35.1.30 igmp-snooping preview permit-times

【command】

igmp-snooping preview permit-times *permit-times-value*

no igmp-snooping preview permit-times

【config-mode】

global configuration mode

【parameter】

permit-times-value: the number of multicast previews, in the range of 1-10, the default value is 5.

【description】

igmp-snooping preview permit-times the command is used to configure the number of multicast previews.

no igmp-snooping preview permit-times command is used to return to default.

Number of times the multicast group is online.

【example】

#configure the multicast preview count to 2

Switch#configure terminal

Switch(config)#igmp-snooping preview permit-times 2

35.1.31 igmp-snooping preview time-reset

【command】

igmp-snooping preview time-reset *time-reset-value*

no igmp-snooping preview time-reset

【config-mode】

global configuration mode

【parameter】

time-reset-value: The length of multicast preview reset, in the range of 1800-7200, in seconds, the default value is 3600.

【description】

igmp-snooping preview time-reset command is used to configure the time length of multicast preview reset.

no igmp-snooping preview time-reset command is used to return to default.

When the reset time is reached, the multicast group restarts the process of iterating from online to offline state.

【example】

#configure the multicast preview reset time to 1800 seconds.

Switch#configure terminal

Switch(config)#igmp-snooping preview time-reset 1800

35.1.32 igmp-snooping profile

【command】

igmp-snooping profile *profile-id*

no igmp-snooping profile [*profile-id*]

【config-mode】

global configuration mode

【parameter】

profile-id: profile ID, the value range is 1-128.

【description】

igmp-snooping profile command to create a profile and enter profile configuration mode.

no igmp-snooping profile command to delete a profile.

【example】

#create profile 1

Switch#configure terminal

Switch(config)#igmp-snooping profile 1

35.1.33 profile limit

【command】

profile limit { permit | deny }

【config-mode】

profile configuration mode

【parameter】

permit: represents allow learning, default configuration.

deny: expresses refusal to learn.

【description】

profile limit { permit | deny } command is used to configure the filter type.

When the profile filter type is permit, only multicast groups in the specified range are allowed to learn; when the filter type is deny, only multicast groups other than the specified range are allowed to learn.

【example】

#configure the filter type of profile 1 to deny

Switch#configure terminal

Switch(config)#igmp-snooping profile 1

Switch(config-igmp-profile-1)#profile limit deny

35.1.34 ip range

【command】

ip range *start-ip-address end-ip-address* **[vlan** *vlan-id* **]**

no ip range *start-ip-address end-ip-address* **[vlan** *vlan-id* **]**

【config-mode】

profile configuration mode

【parameter】

start-ip-address: starting IP address, dotted decimal, e.g.: 225.0.0.2.

end-ip-address: ending IP address, dotted decimal, e.g.: 225.0.0.4.

vlan-id: VLAN ID value, the value range is 1-4094.

【description】

ip range command is used to configure the IP address segment.

no ip range command is used to disable the configuration of IP address segments.

【example】

#configure profile 1 to add the IP address segment 225.0.0.2-225.0.0.4 and to belong to VLAN 2

Switch#configure terminal

Switch(config)#igmp-snooping profile 1

Switch(config-igmp-profile-1)#ip range 225.0.0.2 225.0.0.4 vlan 2

35.1.35 mac range

【command】

mac range *start-mac-address end-mac-address* **[vlan** *vlan-id* **]**

no mac range *start-mac-address end-mac-address* **[vlan** *vlan-id* **]**

【config-mode】

profile configuration mode

【parameter】

start-mac-address: start MAC address, colon divided into hexadecimal, such as: 01::00:5e:00:00:02.

end-mac-address: ending MAC address, colon divided into hexadecimal, such as: 01::00:5e:00:00:04.

vlan-id: VLAN ID value, value range is 1-4094.

【description】

mac range command is used to configure the MAC address segment.

no mac range command is used to unconfigure the MAC address segment.

【example】

#configure profile 1 to add MAC address segment 01:00:5e:00:00:02-01:00:5e:00:00:04 and belong to VLAN 2

Switch#configure terminal

Switch(config)#igmp-snooping profile 1

Switch(config-igmp-profile-1)#mac range 01:00:5e:00:00:02 01:00:5e:00:00:04 vlan 2

35.1.36 description

【command】

description *description-value*

no description

【config-mode】

global configuration mode

【parameter】

description-value: description information of the profile, up to 32 characters.

【description】

description command is used to configure profile description information.

no description command to unconfigure profile description information.

【example】

#configure profile 1 description information to Profile1

Switch#configure terminal

Switch(config)#igmp-snooping profile 1

Switch(config-igmp-profile-1)#description Profile1

35.1.37 igmp-snooping profile refer

【command】

igmp-snooping profile refer *profile-id*

no igmp-snooping profile refer [*profile-id***]**

【config-mode】

port \ VLAN configuration mode

【parameter】

profile-id: profile ID, the value range is 1-128.

【description】

igmp-snooping profile refer command is used to configure the application profile.

no igmp-snooping profile refer command is used to unconfigure the application profile.

【example】

#configure port ethernet 0/0/1 to apply profile 1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#igmp-snooping profile refer 1

35.1.38 igmp-snooping { permit | deny } group all

【command】

igmp-snooping { permit | deny } group all

【config-mode】

global configuration mode

【parameter】

none

【description】

igmp-snooping permit group all command is used to allow learning of all multicast groups.

igmp-snooping deny group all command is used to refuse to learn all multicast groups.

By default, all multicast groups are allowed to be learned.

【example】

#configure deny learning for all multicast groups.

Switch#configure terminal

Switch(config)#igmp-snooping deny group all

35.1.39 igmp-snooping { permit | deny } { group | group-range }

【command】

igmp-snooping {permit | deny} {group *mac-address* **| group-range** *mac-address* **multi-count** *count-value***} vlan** *vlan-id*

no igmp-snooping {permit | deny} group [*mac-address* **vlan** *vlan-id***]**

【config-mode】

port Configuration Modess

【parameter】

mac-address: multicast group MAC address value, colon divided into hexadecimal, such as: 01:00:5e:00:00:01.

count-value: the number of multicast groups, in the range of 1 to 64.

vlan-id: VLAN ID value, the value range is 1-4094.

【description】

igmp-snooping {permit | deny} command is used to configure the black and white list.

no igmp-snooping {permit | deny} command is used to unconfigure the black and white list.

permit is used to configure whitelist, deny is used to configure blacklist.

When the global configuration permit group all, the port configuration blacklist is valid;

When the global configuration deny group all, the port configuration whitelist is valid.

【example】

#configure the whitelist 01:00:5e:00:00:01 under port ethernet 0/0/1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#igmp-snooping permit group 01:00:5e:00:00:01 vlan 1

35.2 IGMP-snooping monitoring and debugging commands

35.2.1 clear igmp-snooping statistics

【command】

clear igmp-snooping statistics [vlan *vlan-id* **| ethernet** *port-id* **]**

【config-mode】

global configuration mode

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

port-id: Port ID value, format stack number/slot number/port number, e.g., 0/0/1.

【description】

clear igmp-snooping statistics command to clear IGMP protocol message statistics.

【example】

#clear the protocol message statistics for VLAN 1 and 2.

Switch#configure terminal

Switch(config)#clear igmp-snooping statistics vlan 1,2

35.2.2 show igmp-snooping

【command】

show igmp-snooping

【config-mode】

arbitrary configuration mode

【parameter】

none

【description】

show igmp-snooping command is used to view the configuration of IGMP Snooping.

【example】

#view the configuration of igmp-snooping.

Switch#configure terminal

Switch(config)#show igmp-snooping

Disable IGMP-Snooping

Disable IGMP-Snooping proxy

Disable IGMP-Snooping static group proxy

Enable IGMP-Snooping query proxy

Proxy Source IP 0.0.0.0

Forwarding-mode is MAC

The max response time is 10 second(s)

The host port timeout is 0 second(s).

Disable IGMP-Snooping route-port forward

The Router port timeout is 300 second(s), Currently aging is stop

Denied VLAN:

1-4094

Black list:

NULL

White list:

NULL

Default group policy is permit

IGMP-Snooping Querier : OFF

IGMP-Snooping Querier Election : ON

Querier vlan : 1

Querier Source IP 0.0.0.0 | Query interval 125 sec | Special query interval 1

sec | Robust count 2 | IGMP-Snooping version 2

Port Information:

port limit overflow fast-leave mcast-vlan igmp-profile drop-pkt

e0/0/1 100 drop enabled 100 1 query

e0/0/2 1024 drop disabled disabled disabled null

e0/0/3 1024 drop disabled disabled disabled null

show igmp-snooping display field description

Fields	Description
Proxy Source IP	Query the source IP used by the proxy
Forwarding-mode	Forwarding mode
The max response time	Maximum response time for generic group query messages
The host port timeout	Aging time of multicast member ports
Denied VLAN	List of VLANs that are not enabled for IGMP Snooping
Black list	Multicast Group Blacklist

White list	Multicast group whitelist
IGMP-Snooping Querier	Queryer enable state
IGMP-Snooping Querier Election	Queryer election enable state
Querier vlan	Query VLAN List
Querier Source IP	Query the source IP of the message
Query interval	Generic group query interval
Special query interval	Group-specific query interval
Robust count	Number of queries for a particular group
IGMP-Snooping version	Protocol Version
port	Port number
limit	Maximum number of multicast groups that can be learned
overflow	Overflow handling actions: drop, replace
fast-leave	Quickly leave the enable state
mcast-vlan	Multicast VLAN
igmp-profile	The profile ID of the application
drop-pkt	Discarded protocol message types: query, report

35.2.3 show igmp-snooping mcast-table

【command】

show igmp-snooping mcast-table [ip-address *ip-address*| **ethernet** *port-id*]

【config-mode】

arbitrary configuration mode

【parameter】

ip-address: multicast group IP address, dotted decimal, e.g., 225.0.0.1.

port-id: port ID value, format: stack number/slot number/port number, e.g., 0/0/1.

【description】

show igmp-snooping mcast-table command to view IGMP Snooping dynamic multicast member table entries.

【example】

#view IGMP snooping dynamic member table entries.

Switch#configure terminal

Switch(config)#show igmp-snooping mcast-table

Show IGMP-snooping multicast table:

Vlan ID: 1, Group IP: 225.0.0.1

Port: e0/0/8, Filter Mode: exclude, Static: false

Expire: 253, V1 Expire: 0, V2 Expire: 253, V3 Expire: 0

Forward Source(0): N/A

Block Source(0) : N/A

show igmp-snooping mcast-table display field description

Field	Description

Vlan ID	VLAN ID of the member port
Group IP	IP address of the joined multicast group
Port	Member Port
Filter Mode	Filter mode
Static	Whether it is a static member or not
Expire	Aging time
VI Expire	IGMPv1 member aging time
V2 Expire	IGMPv2 member aging time
V3 Expire	IGMPv3 member aging time
Forward Source(0)	IGMPv3 Multicast Source Whitelist
Block Source(0)	IGMPv3 Multicast Source Blacklist

35.2.4 show igmp-snooping static-table

【command】

show igmp-snooping static-table

【parameter】

arbitrary configuration mode

【description】

none

【description】

show igmp-snooping static-table command to view IGMP Snooping static multicast member table entries.

【example】

#vew IGMP snooping static member table entries.

Switch#configure terminal

Switch(config)#show igmp-snooping static-table

Show IGMP-snooping static multicast table:

Vlan ID: 1, Group IP: 225.0.0.2

Port: e0/0/1, Filter Mode: exclude, Static: true

Expire: 0, V1 Expire: 0, V2 Expire: 0, V3 Expire: 0

Forward Source(0): N/A

Block Source(0) : N/A

show igmp-snooping static-table View field descriptions

Fields	Description
Vlan ID	VLAN ID of the member port
Group IP	IP address of the joined multicast group
Port	Member Port
Filter Mode	Filter mode
Static	Whether it is a static member

Expire	Aging time
VI Expire	IGMPv1 member aging time
V2 Expire	IGMPv2 member aging time
V3 Expire	IGMPv3 member aging time
Forward Source(0)	IGMPv3 Multicast Source Whitelist
Block Source(0)	IGMPv3 Multicast Source Blacklist

35.2.5 show igmp-snooping fib-table

【command】

show igmp-snooping fib-table

【config-mode】

arbitrary configuration mode

【parameter】

none

【description】

show igmp-snooping fib-table command to view multicast hardware forwarding table.

【example】

#view IGMP snooping multicast member hardware forwarding table entries.

Switch#configure terminal

Switch(config)#show igmp-snooping fib-table

Show IGMP-snooping multicast forward table:

VLAN (Source, Group) Interface

1 (*, 225.0.0.1) e0/0/8.

1 (*, 225.0.0.2) e0/0/1.

show igmp-snooping fib-table displays field descriptions

Fields	Description
VLAN	VLAN ID of the forwarding table entry
(Source, Group)	(source, group)
Interface	Port number

35.2.6 show igmp-snooping router-dynamic

【command】

show igmp-snooping router-dynamic

【config-mode】

arbitrary configuration mode

【parameter】

none

【description】

show igmp-snooping router-dynamic command to view the dynamic router port list.

【example】

#View IGMP snooping dynamic routing ports.

Switch#configure terminal

Switch(config)#show igmp-snooping router-dynamic

VlanID PortID Expire(Second)

1 e0/0/8 300

show igmp-snooping router-dynamic Show field description

Fields	Description
VlanID	VLAN to which the router port belongs
PortID	Router port number
Expire(Second)	Routing port aging time (seconds)

35.2.7 show igmp-snooping router-static

【command】

show igmp-snooping router-static [vlan *vlan-id* **| ethernet** *port-id***]**

【config-mode】

arbitrary configuration mode

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

port-id: port ID, format: stacking number/slot number/port number, e.g., 0/0/1.

【description】

show igmp-snooping router-static command to view static router ports.

【example】

#view IGMP snooping static route port.

Switch#configure terminal

Switch(config)#show igmp-snooping router-static

VlanID PortList

1 e0/0/1.

show igmp-snooping router-static Show field description

Fields	Description
VlanID	VLAN to which the router port belongs
PortList	Router Port List

35.2.8 show igmp-snooping preview

【command】

show igmp-snooping preview

【config-mode】

arbitrary configuration mode

【parameter】

none

【description】

show igmp-snooping preview command is used to view the multicast preview configuration.

【example】

#view Multicast Preview Configuration.

Switch#configure terminal

Switch(config)#show igmp-snooping preview

preview switch : enable

preview time-once : 180

preview time-interval: 300

preview time-reset : 3600

preview permit-times : 5

MulticastIP MulticastVlan Port

225.0.0.1 1 e0/0/8

show igmp-snooping preview display field description

Fields	Description
preview switch	Multicast preview enable state
preview time-once	Multicast Preview Duration
preview time-interval	Multicast preview interval
preview time-reset	Multicast Preview Reset Time
preview permit-times	Number of multicast previews
MulticastIP	Multicast groups
MulticastVlan	Belonging VLAN
Port	Member Port

35.2.9 show igmp-snooping preview status

【command】

show igmp-snooping preview status

【config-mode】

arbitrary configuration mode

【parameter】

none

【description】

show igmp-snooping preview status command to view the member port status of the multicast preview group.

【example】

#view the member port status information of IGMP Snooping multicast preview group.

Switch#configure terminal

Switch(config)#show igmp-snooping preview status

MulticastIP MulticastVlan Port PreviewTimes Online

225.0.0.1 1 e0/0/8 0 N

show igmp-snooping preview status showing field descriptions

Fields	Description
MulticastIP	Preview Multicast Groups
MulticastVlan	Preview the VLAN to which the multicast group belongs
Port	Preview multicast group member port numbers
PreviewTimes	Preview the number of times the multicast group is currently located
Online	Previewing the current state of a multicast group

35.2.10 show igmp-snooping profile

【command】

show igmp-snooping profile [*profile-id*]

【config-mode】

arbitrary configuration mode

【parameter】

profile-id: profile ID, the value range is 1-128.

【description】

show igmp-snooping profile the command is used to view the filter index file configuration information.

【example】

#view the configuration information of IGMP Snooping filter index file 1.

Switch#configure terminal

Switch(config)#show igmp-snooping profile 1

IGMP-Snooping profile 1

Profile description : profile1

Profile limit : permit

Profile referred : e0/0/1.

start-address end-address vlan

225.0.0.5 225.0.0.6 any

01:00:5e:00:00:07 01:00:5e:00:00:08 any

01:00:5e:00:00:09 01:00:5e:00:00:0a 1

Total ip range: 1, mac range: 2

show igmp-snooping profile View field descriptions

Fields	Description

Profile description	Description Information
Profile limit	Filter Type
Profile referred	Cited information
start-address	Address segment start address
end-address	Address segment end address
vlan	Address segment appointed VLAN

35.2.11 show igmp-snooping profile ethernet

【command】

show igmp-snooping profile ethernet *port-id* **[to ethernet** *port-id***]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: port ID value, format: stack number/slot number/port number, e.g., 0/0/1.

【description】

show igmp-snooping profile ethernet command is used to view the configuration contents of the port application filter file.

【example】

#view the application of port 1 to profile.

Switch#configure terminal

Switch(config)#show igmp-snooping profile ethernet 0/0/1

Interface e0/0/1

Profile limit: permit

Profile refer: 1

profile	start-address	end-address	vlan
1	225.0.0.5	225.0.0.6	any
1	01:00:5e:00:00:07	01:00:5e:00:00:08	any
1	01:00:5e:00:00:09	01:00:5e:00:00:0a	1

Total ip range: 1, mac range: 2

show igmp-snooping profile ethernet View field description

Fields	Description
Interface	Port number
Profile limit	restriction type
Profile refer	Filter file ID of the application
profile	Filter File ID
start-address	Address segment start address
end-address	Address segment end address
vlan	Address segment to assign a VLAN

35.2.12 show igmp-snooping profile vlan

【command】

show igmp-snooping profile vlan *vlan-id*

【config-mode】

arbitrary configuration mode

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

【description】

show igmp-snooping profile vlan command is used to view the configuration content of the VLAN application filter file.

【example】

#view the application of VLAN1 to the filter file.

Switch#configure terminal

Switch(config)#show igmp-snooping profile vlan 1

Vlan information of profile

Vlan 1

Profile limit: deny

Profile refer: 2

profile start-address end-address

2 225.0.0.3 225.0.0.4

Total ip range: 1, mac range: 0

show igmp-snooping profile vlan display field description

Fields	Description
Vlan	VLAN number
Profile limit	Restriction Type
Profile refer	Filter file ID of the application

profile	Filter File ID
start-address	Address segment start address
end-address	Address segment end address

35.2.13 show igmp-snooping statistics

【command】

show igmp-snooping statistics {**all** | **vlan** *vlan-id*| **ethernet** *port-id*}

【config-mode】

arbitrary configuration mode

【parameter】

vlan-id: VLAN ID value, value range is 1-4094.

port-id: Port ID, format: stack number/slot number/port number, e.g., 0/0/1.

【description】

show igmp-snooping statistics command is used to view the protocol message statistics.

【example】

#view protocol message statistics for VLAN 1.

Switch#configure terminal

Switch(config)#show igmp-snooping statistics vlan 1

Vlan 1 statistics : Rx Tx

IGMPv1 general query : 0 0

IGMPv2 general query : 6705 6930

IGMPv2 spec group query : 50 0

IGMPv3 general query : 0 0

IGMPv3 spec group query : 0 0

IGMPv3 spec src group query: 0 0

IGMPv1 report : 0 0

IGMPv2 report : 23 23

IGMPv3 report : 0 0

IGMPv2 leave : 0 0

Invalid query : 53 0

Invalid report : 0 0

Invalid leave : 0 0

Invalid packet : 17 0

DVMRP probe : 0 0

DVMRP other packet : 0 0

PIM hello : 0 0

PIM other packet : 0 0

show igmp-snooping statistics showing field descriptions

Fields	Description
IGMPv1 general query	IGMPv1 generic group query message
IGMPv2 general query	IGMPv2 generic group query message
IGMPv2 spec group query	IGMPv2 group-specific query message
IGMPv3 general query	IGMPv3 generic group query message

IGMPv3 spec group query	IGMPv3 group-specific query message
IGMPv3 spec src group query	IGMPv3 source-specific group-specific query packets
IGMPv1 report	IGMPv1 report message
IGMPv2 report	IGMPv2 report message
IGMPv3 report	IGMPv3 report message
IGMPv2 leave	IGMPv2 leave message
Invalid query	Invalid IGMP query message
Invalid report	Invalid IGMP report message
Invalid leave	Invalid IGMP leave message
Invalid packet	Invalid packets
DVMRP probe	DVMRP Probe packets
DVMRP other packet	DVMRP Other packets
PIM hello	PIM hello packet
PIM other packet	PIM other packets
Rx	Total number of packets received
Tx	Total number of packets sent

35.2.14 debug igmp_snooping

【command】

debug igmp_snooping

no debug igmp_snooping

【config-mode】

global configuration mode

【parameter】

none

【description】

debug igmp_snooping command to enable IGMP Snooping debug switch.

no debug igmp_snooping command to turn off IGMP Snooping debug switch.

By default, the IGMP Snooping debug switch is not enabled.

【example】

#enable IGMP Snooping debug switch

Switch#configure terminal

Switch(config)#debug igmp_snooping

Chapter 36 IPv4 Multicast Basics

36.1 IPv4 multicast basic configuration commands

36.1.1 ip multicast-routing

【command】

ip multicast-routing

no ip multicast-routing

【config-mode】

global configuration mode

【parameter】

none

【description】

ip multicast-routing the command enables the Layer 3 multicast forwarding function.

no ip multicast-routing the command is used to disable the Layer 3 multicast forwarding function.

By default, the Layer 3 multicast forwarding function is not enabled.

【example】

#enable multicast forwarding function.

Switch#configure terminal

Switch(config)#ip multicast-routing

36.1.2 mroute igmp

【command】

mroute igmp

【config-mode】

global configuration mode

【parameter】

none

【description】

mroute igmp command to enter IGMP configuration mode.

【example】

#Enter IGMP configuration mode.

Switch#configure terminal

Switch(config)#mroute igmp

Switch(config-router-igmp)#

36.1.3 mroute pim

【command】

mroute pim

【config-mode】

global configuration mode

【parameter】

none

【description】

mroute pim command is used to enter PIM configuration mode.

【example】

#enter PIM configuration mode.

Switch#configure terminal

Switch(config)#mroute pim

Switch(config-router-pim)#

Chapter 37 IPv6 Multicast Basics

37.1 IPv6 Multicast Basic Configuration Commands

37.1.1 multicast mac-address vlan

【command】

multicast mac-address *mac-address* **vlan** *vlan-id*

no multicast mac-address *mac-address* **vlan** *vlan-id*

【config-mode】

global configuration mode

【parameter】

mac-address: MAC address, bubble minute sixteen system format, such as: 33:33:00:00:00:00:01.

vlan-id: VLAN ID value, value range is 1-4094.

【description】

multicast mac-address vlan command is used to configure Layer 2 static multicast table entries.

no multicast mac-address The command deletes the Layer 2 static multicast table entry.

By default, no Layer 2 static multicast table entry is configured.

Instructions:

⇌ The configured MAC address must be a legal multicast MAC address, not a broadcast or unicast.

【example】

#Configure static multicast table entry 33:33:00:00:00:01 vlan 1.

Switch#configure terminal

Switch(config)#multicast mac-address 33:33:00:00:00:01 vlan 1

37.1.2 multicast mac-address vlan interface

【command】

multicast mac-address *mac-address* **vlan** *vlan-id* **interface { all | ethernet** *port-id* **}**

no multicast mac-address *mac-address* **vlan** *vlan-id* **interface { all | ethernet** *port-id* **}**

【config-mode】

global configuration mode

【parameter】

mac-address: MAC address, adventitious hex format, such as: 33:33:00:00:00:00:01.

vlan-id: VLAN ID value, the value range is 1-4094.

all: represents all ports.

port-id: Port ID value, format stack number/slot number/port number, e.g., 0/0/1.

【description】

multicast mac-address vlan interface The command is used to configure two groups of static multicast member ports.

no multicast mac-address vlan interface Command to delete a Layer 2 static multicast member port.

By default, no Layer 2 static multicast member port is configured.

【example】

#Configure member port ethernet 0/0/1 for static multicast 33:33:00:00:00:01.

Switch#configure terminal

Switch(config)#multicast mac-address 33:33:00:00:00:01 vlan 1

Switch(config)#multicast mac-address 33:33:00:00:00:01 vlan 1 interface ethernet 0/0/1

37.2 IPv6 Multicast Basic Monitoring and Debugging Commands

37.2.1 show multicast mld-snooping

【command】

show multicast mld-snooping

【config-mode】

arbitrary configuration mode

【parameter】

none

【description】

show multicast mld-snooping Command to view IPv6 multicast table entries.

【example】

#view IPv6 multicast forwarding table entries.

Switch#configure terminal

Switch(config)#show multicast mld-snooping

show multicast table information

MAC Address : 33:33:00:00:00:01

VLAN ID : 1

Static port list : e0/0/1.

MLD port list : e0/0/18.

show multicast mld-snooping Show field descriptions

Fields	Description
MAC Address	Multicast MAC address
VLAN ID	VLAN to which the multicast belongs
Static port list	Multicast static member ports
MLD port list	Multicast dynamic member port list

37.2.2 debug multicast

【command】

debug multicast

no debug multicast

【config-mode】

global configuration mode

【parameter】

none

【description】

debug multicast The command enables the Layer 2 multicast debug switch.

no debug multicast Command to turn off the Layer 2 multicast debug switch.

【example】

#Enable multicast debugging function

Switch#configure terminal

Switch(config)#debug multicast

Chapter 38 CoS

38.1 CoS configure command

38.1.1 queue-scheduler group-id strict-priority

【command】

queue-scheduler *group-id* **strict-priority**

no queue-scheduler [*group-id* **]**

【config-mode】

Global configuration mode

【parameter】

group-id: Group number,integer format,fixed value 1.

【description】

queue-scheduler *group-id* **strict-priority** ;Command is used to configure the queue scheduling mode as SP.

no queue-scheduler [*group-id* **]** ;Command is used to restore the default configuration. In default, the scheduling mode is SP.

Notes:

Queue scheduling only works when the network congestion occurs.

【example】

#Configure the queue scheduling mode as SP.

switch#configure terminal

switch (config)#queue-scheduler 1 strict-priority

38.1.2 queue-scheduler group-id wfq

【command】

queue-scheduler *group-id* **wfq** *weight1 weight2 weight3…weight8*

no queue-scheduler [*group-id* **]**

【config-mode】

Global configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

weight1～*weight8*：Weight value, integer format, value range 1-100.

【description】

queue-scheduler *group-id* **wfq** *weight1 weight2 weight3…weight8*; Command is used to configure the queue scheduling mode as wfq.

no queue-scheduler; Command is used to restore the default configuration. In default, the scheduling mode is SP.

【example】

#Configure the WFQ scheduling policy, and the queue allocation weights are 1:1:1:1:1:1:1:1。

switch#configure terminal

switch(config)#queue-scheduler 1 wfq 1 1 1 1 1 1 1 1

38.1.3 queue-scheduler group-id sp-wfq

【command】

queue-scheduler *group-id* **sp-wfq** *weight1 weight2 weight3…weight8*

no queue-scheduler [*group-id* **]**

【config-mode】

Global Configuration Mode

【parameter】

group-id：Group number, integer format, fixed value 1.

weight1～*weight8*：The weight value, integer format, value range 0-100.

【description】

queue-scheduler *group-id* **sp-wfq** *weight1 weight2 weight3…weight8*; Command is used to configure the queue scheduling mode as sp-wfq.

no queue-scheduler [*group-id* **]**; Command is used to restore the default configuration. In default, the scheduling mode is SP.

The SP + WFQ is implemented as follows：And 0 was used as the split point，Divided into 3 cohorts：{w1} 、{0} 、{w3}，{w3}The priority is highest，{w1}The priority is second，{0}The priority is lowest..Each queue in {w3} and {w1} forwards according to the weight ratio.

【example】

Configure the sp-wfq scheduling strategy with the queue allocation weights of 1:2:3:4:5:0:7:8.

switch#configure terminal

switch(config)#queue-scheduler 1 sp-wfq 1:2:3:4:5:0:7:8

38.1.4 queue-scheduler group-id wrr

【command】

queue-scheduler *group-id* **wrr** *weight1 weight2 weight3…weight8*

no queue-scheduler [*group-id* **]**

【config-mode】

Global configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

weight1～weight8：Weight value, integer format, value range 1-100.

【description】

queue-scheduler *group-id* **wrr** *weight1 weight2 weight3…weight8*;Command is used to configure the queue scheduling mode as wrr.

no queue-scheduler [*group-id* **]**; Command is used to restore the default configuration. In default, the scheduling mode is SP.

【example】

#Using the wrr scheduling policy, the queue allocation weights are 1:1:1:1:1:1:1:1.

switch#configure terminal

switch(config)#queue-scheduler 1 wrr 1 1 1 1 1 1 1 1

38.1.5 queue-scheduler group-id sp-wrr

【command】

queue-scheduler *group-id* **sp-wrr** *weight1 weight2 weight3…weight8*

no queue-scheduler [*group-id* **]**

【config-mode】

Global configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

weight1～*weight8*：Weight value, integer format, value range 0-100.

【description】

queue-scheduler *group-id* **sp-wrr** *weight1 weight2 weight3…weight8*;Command is used to configure the queue scheduling mode as sp-wrr

no queue-scheduler [*group-id* **]**; Command is used to restore the default configuration. In default, the scheduling mode is SP.

The SP + WRP is implemented as follows: 0 is taken as the segmentation point and divided into three queues: {w1}, {0}, {w3}, {w3} has the highest priority, {w1} has the second priority, and {0} has the lowest priority. Each queue in {w3} and {w1} forwards according to the weight ratio.

【example】

#Using the sp-wrr scheduling policy, the queue allocation weights are 1:2:3:4:5:0:7:8

switch#configure terminal

switch(config)#queue-scheduler 1 sp-wrr 1:2:3:4:5:0:7:8

38.1.6 queue-scheduler cos-map group-id priority queue

【command】

queue-scheduler cos-map *group-id priority queue*

no queue-scheduler [*group-id* **]**

【config-mode】

Global configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

priority：Message priority, integer format, value range 0-7.

queue：Hardware queue number, integer format, value range 0-7.

【description】

queue-scheduler cos-map *group-id priority queue*;Command is used to configure priority priority with hardware queue queue mapping.

no queue-scheduler [*group-id* **]**; Command is used to restore the default configuration. In default, , the priority 0-7 maps with the hardware queue 0-7 separately.

【example】

#Configure that the priority 1 maps to the hardware queue 2.

switch#configure terminal

switch(config)# queue-scheduler cos-map 1 1 2

38.1.7 queue-scheduler cos-map group-id

【command】

queue-scheduler cos-map *group-id*

【config-mode】

Port configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

【description】

queue-scheduler cos-map *group-id*; Command is used to configure the queue group for cos-map.

This command is optional.because only supports queue group 1, and it is default configureation and can not be closed.

【example】

Configure port 0 / 0 / 1 cos-map to run Queue Group 1.

switch #configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#queue-scheduler cos-map 1

38.1.8 queue-scheduler dscp-map

【command】

queue-scheduler dscp-map

no queue-scheduler dscp-map

【config-mode】

Global configuration mode

【parameter】

None

【description】

queue-scheduler dscp-map; Enable the dscp-map function.

no queue-scheduler dscp-map; Disable the dscp-map function.

By default, the dscp-map function is disabled.

Notes:

The dscp-map is mutually exclusive with the VLAN priority of the packet, and the dscp-map is higher than the VLAN

priority of the packet. Even after the dscp-map, the queue scheduling will not forward according to the VLAN priority of the packet. One message carries both vlan priority p1 and dscp d1, and the queue scheduling process is as follows:

1. After enable the dscp-map function, the system extracts the dscp d1 in the IP head, then looks up the dscp d1 map priority p from the dscp-map table item, then looks up the queue q of the priority p map from the cos-map, and finally forwards according to the queue q.(No own vlan priority p1 is used during the whole process)

2. After disable dscp-map function, the system extracts the priority p1 in the VLAN header, then looks up the priority p1 mapping queue q from the cos-map, and finally forwards according to the queue q.(dscp d1 is not used during the whole process)

【example】

#Enable the dscp-map function

switch#configure terminal

switch(config)#queue-scheduler dscp-map

38.1.9 queue-scheduler dscp-map group-id dscp priority

【command】

queue-scheduler dscp-map *group-id dscp-value queue*

no queue-scheduler dscp-map

【config-mode】

Global configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

dscp-value：The dscp value, integer format, value range 0-63.

queue：Queue number, integer format, value range 0-7.

【description】

queue-scheduler dscp-map *group-id dscp-value queue*; Command is used to configure the dscp and the priority mapping relationships.

the dscp-map function must enable before configuration.

【example】

#Configure dscp 10 mapping to priority 0.

switch #configure terminal

switch(config)#queue-scheduler dscp-map

switch(config)#queue-scheduler dscp-map 1 10 0

38.1.10 queue-scheduler group-id

【command】

queue-scheduler *group-id*

【config-mode】

Port configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

【description】

queue-scheduler *group-id*；Command the queue-scheduler group number.

This command is optional.because only supports queue group 1, and it is default configureation and can not be closed.

【example】

#Configure port 0/0/1 run Queue group 1.

switch #configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#queue-scheduler 1

38.1.11 queue-scheduler dscp-map group-id

【command】

queue-scheduler dscp-map *group-id*

【config-mode】

Global configuration mode

【parameter】

group-id：Group number, integer format, fixed value 1.

【description】

queue-scheduler dscp-map *group-id*; Command is used to configure the queue group number for dscp-map.

This command is optional.because only supports queue group 1, and it is default configuration and can not be closed.

【example】

#Configure port 0/0/1 dscp-map to run Queue group 1.

switch #configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#queue-scheduler dscp-map 1

38.2 CoS Monitoring and debugging command

38.2.1 show queue-scheduler

【command】

show queue-scheduler [*group-id* **]**

【config-mode】

Global configuration mode

【parameter】

group-id: Group number, integer format, fixed value of 1.

【description】

show queue-scheduler *group-id*; Command is used show queue-scheduler configuration.

【example】

#View the queue scheduler configuration information.

switch#configure terminal

switch (config)#show queue-scheduler

Queue scheduler status : enable

Queue scheduler mode : SP (Strict Priority)

show queue-scheduler display field description

field	instruction
Queue scheduler status	Queue scheduler function status: enable, disable
Queue scheduler mode	mode : sp, wrr, sp-wrr, wfq, sp-wfq

38.2.2 show queue-scheduler cos-map

【command】

show queue-scheduler cos-map [*group-id* **]**

【config-mode】

Global configuration mode

【parameter】

group-id: Group number,integer format, fixed value 1.

【description】

show queue-scheduler cos-map [*group-id* **]**; Command is used to view cos-map configuration.

【example】

#View the cos-map configuration information.

switch#configure terminal

switch(config)#show queue-scheduler cos-map

Information about map of cos:

802.1P Priority Queue of class

group 1----------

0 0

1 1

2 2

3 3

4 4

5 5

6 6

7 7

show queue-scheduler cos-map display field description

field	instruction
802.1P Priority	Priority: 0-7
Queue of class	Hardware queue number: 0-7

38.2.3 show queue-scheduler dscp-map

【command】

show queue-scheduler dscp-map [*group-id*]

【config-mode】

Global configuration mode

【parameter】

group-id: Group number, integer format, fixed value 1.

【description】

show queue-scheduler dscp-map [*group-id*]; Command is used to show dscp-map information.

【example】

#View the dscp-map configuration information.

switch#configure terminal

switch(config)#show queue-scheduler dscp-map

Information about map of dscp:

DSCP value 802.1P Priority

---

0 0

1 0

2 0

3 0

4 0

5 0

6 0

7 0

8 1

9 1

10 1

11 1

12 1

13 1

14 1

15 1

16 2

……

show queue-scheduler cos-map display field description

field	instruction
DSCP value	dscp
802.1P Priority	VLAN priority

38.2.4 show queue-scheduler port-map

【command】

show queue-scheduler port-map

【config-mode】

Global configuration mode

【parameter】

None

【description】

show queue-scheduler port-map; Command is used to show port queue configuration.

【example】

#View the port queue scheduling information

switch#show queue-scheduler port-map

port 0/0/1 scheduler:1 cos-map:1 dscp-map:1

port 0/0/2 scheduler:1 cos-map:1 dscp-map:1

port 0/0/3 scheduler:1 cos-map:1 dscp-map:1

port 0/0/4 scheduler:1 cos-map:1 dscp-map:1

port 0/0/5 scheduler:1 cos-map:1 dscp-map:1

port 0/0/6 scheduler:1 cos-map:1 dscp-map:1

port 0/0/7 scheduler:1 cos-map:1 dscp-map:1

port 0/0/8 scheduler:1 cos-map:1 dscp-map:1

port 0/0/9 scheduler:1 cos-map:1 dscp-map:1

……

show queue-scheduler cos-map display field description

field	instruction
scheduler 1	Queue group number, fixed value 1
cos-map 1	cos-map group number, fixed value 1
dscp-map 1	dscp-map group number, fixed value 1

Chapter 39 ACL

39.1 ACL configure command

39.1.1 access-list acl-id match-order

【command】

access-list *acl-id* **match-order [auto | config]**

【config-mode】

Global configuration mode

【parameter】

acl-id: Access control list number, integer format, value range 1-2999.

auto: It represents automatic priority according to depth, deep row and shallow row.

config: It means the use of configuration sequence sorting, first configuration row, after configuration row.

【description】

access-list *acl-id* **match-order [auto | config];** Command is used to configure ACL match-order.

Default is auto.

if acl-id already exists,the command can't be configured.

【example】

#Configure access control list 1 match-order is config.

switch#configure terminal

switch(config)#access-list 1 match-order config

39.1.2 access-list step

【command】

access-list step *step*

no access-list step

【config-mode】

Global configuration mode

【parameter】

step：Subitem serial number increase step length, integer format, value range 1-10.

【description】

access-list step *step*; Command is used to configure the ACL subitem increment step size.

no access-list step; Command is used to restore the default configuration.

If one ACL contains multiple subitems, the first subitem number is 0, and the other subitems number will increase step according to the configuration order. By default increment step size is 5.

Notes:

The configuration step does not take effect on existing subitems,but only on newly created subitems in the future. Step only works for children of the same ACL. different ACL subitem are independent. An ACL can contain up to 128 subitems.

【example】

#Configure the ACL subitem step is 10.

switch#configure terminal

switch(config)#access-list step 10

39.1.3 access-list mac-acl-id

【command】

access-list *mac-acl-id* **{ permit | deny } [** *protocol] { source-mac-addr { source-mac-wildcard* **| host } | any }** **{** *destination-mac-addr { destination-mac-wildcard* **| host } | any } [vlan** *vlan-id* **] [cos** *vlan-pri* **] [time-range** *time-range-name* **]**

no access-list { all | *mac-acl-id [subitem-id* **] }**

【config-mode】

Global configuration mode

【parameter】

mac-acl-id：Number of MAC ACL, integer format, value range 1000-1999.

permit：indicates forwarding packet matching ACL.

deny：indicates discarding packet matching ACL.

protocol：Agreement number, hexadecimal format, value range 1-FFFF.

vlan-pri：VLAN Priority, integer form, value range 0-7.

vlan-id：VLAN ID，Integer form, value range 1-4094.

source-mac-addr：Source MAC address, format H: H: H: H: H: H.

destination-mac-addr：Purpose MAC address, format H: H: H: H: H: H.

source-mac-wildcard：source MAC address wildcard mask of the , format ff: ff: ff: ff: ff: ff.

destination-mac-wildcard：destination MAC address wildcard mask, format ff: ff: ff: ff: ff: ff.

host：Represents the host address.

time-range：Indicates the effective time domain of the specified ACL rule.

time-range-name：time range name, string format, supports up to 32 characters.

【description】

access-list *mac-acl-id*; Command is used to configure the MACACL.

no access-list { all | *mac-acl-id [subitem-id* **] }**; Command is used to remove the ACL rules.

【example】

#Deny the packets of the VLAN 4094.

switch#configure terminal

switch(config)#access-list 1000 deny any any 4094

39.1.4 access-list ip-acl-id

【command】

access-list *ip-acl-id* **{ permit | deny } [** *protocol] [icmp-type icmp-code* **] [established] {** *source-ipv4-address { ipv4-mask* **|**

host } | any } [*port-number] { destination-ipv4-address { ipv4-mask* **| host } | any } [** *igmp-type] [port-number* **] [precedence** *precedence* **| tos** *tos* **| dscp** *dscp* **| fragments]* [time-range** *time-range-name* **]**

access-list *ip-acl-id* **{ permit | deny } [** *protocol] [icmp-type icmp-code* **] [established] {** *source-ipv6/M* **| ipv6any }[** *port-number* **] {** *destination-ipv6/M* **| ipv6any } [** *port-number* **] [traffic-class** *traffic-class* **] [time-range** *time-range-name* **]**

no access-list { all | *ip-acl-id [subitem-id* **] }**

【config-mode】

Global configuration mode

【parameter】

ip-acl-id：IP ACL The number, integer format, value range 1-999.

permit：indicates forwarding packet matching ACL.

deny：indicates discarding packet matching ACL.

protocol：Agreement number, support the integer and name format, take the following values:

Integer form, take the value range: 0~255;

name：gre、icmp、icmpv6、igmp、ipinip、ospf、tcp、udp。

source-ipv4-address：Source IPv4 address, point split decimal.

ipv4-mask：The IPv4 address mask.

destination-ipv4-address：Objective IPv4 address, points decimal.

source-ipv6/M：Source IPv6 address and mask length.

destination-ipv6/M：Purpose IPv6 address and mask length.

any：Indicates any IPv4 address.

ipv6any：Indicates any IPv6 address.

icmp：represents the hosting the icmp protocol.

icmpv6：represents the bearer icmpv6 protocol.

icmp-type icmp-code：The icmp type and subtype, only available when the protocol is icmp, icmpv6, supports the integer and name format:

Integer format: value range 0-255;

Name：echo、echo-reply、fragmentneed-dfset、host-redirect、host-tos-redirect、host-unreachable、information-reply、information-request、net-redirect、net-tos-redirect、net-unreachable、parameter-problem、port-unreachable、protocol-unreachable、reassembly-timeout、source-quench、source-route-failed、timestamp-reply、timestamp-request、ttl-exceeded；

udp：represents udp protocol.

tcp：represents tcp protocol.

established：Indicates SYN = 1 in TCP and is only available when the protocol is TCP.

port-number：Transport layer port number, integer form, supports three formats:

Decimal: value range from 1 to 65535

Octal: value range 0-0177777, input starts with 0, automatically converted to decimal when distribution configuration;

Headecimal, value range 0-0xffff, input starts with 0x, automatically converted to decimal when issuing configuration;

wildcard：Transport layer port number wildcard mask.

igmp：Represents igmp protocol.

igmp-type：IGMP protocol type, only available when the protocol is IGMP, integer format, value range:0-34.

precedence：IP priority, support for integer and name format, specifically as follows:

Integer format: value range 0-7;

Name: routine, priority, immediate, flash, flash-override, critical, internet, and network, or value range 0-7.

tos：ToS priority, support integer and name format, with the following values:

Integer format: value range 0-15;

Name: max-reliability (value 2), max-throughput (value 4), min-delay (value 8), min-monetary-co (value 1), normal (value 0).

dscp：DSCP priority, support for integer and name format, specifically as follows:

Integer format: value range 0-63;

Name: af1(10)、af2(18)、af3(26)、af4(34)、cs1(8)、cs2(16)、cs3(24)、cs4(32)、 cs5(40)、cs6(48)、cs7(56)、be(0)、ef(46)

fragments：do not fragmentation: DF=1.

traffic-class：IPv6 priority, integer format, value range 0-63.

time-range-name：The time range name, string format, supports up to 32 characters.

【description】

access-list *ip-acl-num* **{ permit | deny } [** *protocol] [icmp-type icmp-code* **] [established] {** *source-ipv4-address { ipv4-mask* **| host } | any } [** *port-number] { destination-ipv4-address { ipv4-mask* **| host } | any } [** *igmp-type] [port-number* **] [precedence** *precedence* **| tos** *tos* **| dscp** *dscp* **| fragments]* [time-range** *time-range-name* **]** command The ACL rule used to configure the IPV 4 protocol

access-list *ip-acl-num* **{ permit | deny } [** *protocol] [icmp-type icmp-code* **] [established] {** *source-ipv6/M* **| ipv6any }[** *port-number* **] {** *destination-ipv6/M* **| ipv6any } [** *port-number* **] [traffic-class** *traffic-class* **] [time-range** *time-range-name* **]** command The ACL rule used to configure the IPV 6 protocol

no access-list { all | *ip-acl-num [subitem-num*] }command Used to remove the ACL rules.

【example】

#Configuration IP ACL: Discards the ICMP messages.

switch#configure terminal

switch(config)#access-list 1 deny icmp any any

39.1.5 access-list hybrid-acl-id

【command】

access-list *hybrid-acl-id* **{ permit | deny } [** *ip-protocol* **] [vlan** *vlan-id* **] [cos** *vlan-pri* **][src-mac** *src-mac-addr* **{** *mac-wildcard* **| host }] [dst-mac** *dst-mac-addr { mac-wildcard* **| host }] [src-ip** *ip-address { ip-mask* **| any }] [src-port** *port-number* **] [dst-ip** *ip-address { ip-mask* **| any }] [** *igmp-type] [icmp-type icmp-code* **] [dst-port** *port-number* **] [precedence** *precedence* **| tos** *tos* **| dscp** *dscp* **| fragments]*[time-range** *time-range-name* **]**

access-list *hybrid-acl-id* **{ permit | deny } [** *ip-protocol* **] [vlan** *vlan-id* **] [cos** *vlan-pri* **][src-mac** *src-mac-addr* **{** *mac-wildcard* **| host }] [dst-mac** *dst-mac-addr { mac-wildcard* **| host }] [src-ipv6 {** *ipv6-addresss/M* **| ipv6any }] [src-port** *port-number* **] [dst-ipv6 {** *ipv6-addresss/M* **| ipv6any }] [** *igmp-type] [icmp-type icmp-code* **] [dst-port** *port-number* **] [traffic-class** *traffic-class* **] [time-range** *time-range-name* **]**

no access-list { all | *hybrid-acl-id [subitem-id* **] }**

【config-mode】

Global configuration mode

【parameter】

hybrid-acl-id：Hybrid ACL number, integer format, value range 2000-2999.

permit：indicates forwarding packet matching ACL.

deny：indicates discarding packet matching ACL.

ip-protocol：IP layer protocol number, hex-decimal format, value range 1-FFFF.

vlan-pri：VLAN Priority, integer format, value range 0-7.

vlan-id：VLAN ID，Integer format, value range 1-4094.

source-mac-addr：source MAC address, format H: H: H: H: H: H.

destination-mac-addr：destination MAC address, format H: H: H: H: H: H.

mac-wildcard：MAC address wildcard mask, format ff: ff: ff: ff: ff: ff.

host：Represents the host address.

ip-address：IP address, point decimal.

ip-mask：IP address mask.

ipv6-address/M：IPv6 address and mask length.

any：Indicates any IPv4 address.

ipv6any：means any IPv6 address。

icmp-type icmp-code：icmp Type subtype, integer format, value range 0-255, only works when ip-protocol is ICMP or ICMPv6.

port-number：Transport layer port number, integer format, supports three formats:

Decimal: value range 1-65535;

Octal: value range 0-0177777, input starts with 0, automatically converted to decimal when distribution configuration;

Headecimal, value range 0-0xffff, input starts with 0x, automatically converted to decimal when issuing configuration;

Only works when ip-protocol is tcp or udp.

igmp-type：IGMP Protocol , integer format, value range 0-34.

Only works when ip-protocol is IGMP.

precedence：IP priority, support for integer and name format, specific as follows:

Integer format: value range 0-7;

Name: routine, priority, immediate, flash, flash-override, critical, internet, and network, or value range 0-7.

tos：ToS priority, support integer and name format with the following values:

Integer format: value range 0-15;

Name: max-reliability(value 2), max-throughput(value 4), min-delay (value 8), min-monetary-co (value 1), normal (value 0).

dscp：DSCP priority, support for integer and name format, specifically as follows:

Integer format: value range 0-63;

Name: af1(10)、af2(18)、af3(26)、af4(34)、cs1(8)、cs2(16)、cs3(24)、cs4(32)、cs5(40)、 cs6(48)、cs7(56)、be(0)、ef(46);

fragments：do not fragmentation: DF=1.

traffic-class：IPv6 priority, integer form, value range 0-63.

time-range-name：time range name, string format, supports up to 32 characters.

【description】

access-list *hybrid-acl-id* **{ permit | deny } [** *ip-protocol* **] [vlan** *vlan-id* **] [cos** *vlan-pri* **][src-mac** *src-mac-addr* **{** *mac-wildcard* **| host }] [dst-mac** *dst-mac-addr { mac-wildcard* **| host }] [src-ip** *ip-address { ip-mask* **| any }] [src-port** *port-number* **] [dst-ip** *ip-address { ip-mask* **| any }] [** *igmp-type] [icmp-type icmp-code* **] [dst-port** *port-number* **] [precedence** *precedence* **| tos** *tos* **| dscp** *dscp* **| fragments]*[time-range** *time-range-name* **];** Command is used to configure the ipv4 hybrid ACL rules

access-list *hybrid-acl-id* **{ permit | deny } [** *ip-protocol* **] [vlan** *vlan-id* **] [cos** *vlan-pri* **][src-mac** *src-mac-addr* **{** *mac-wildcard* **| host }] [dst-mac** *dst-mac-addr { mac-wildcard* **| host }] [src-ipv6 {** *ipv6-addresss/M* **| ipv6any }] [src-port** *port-number* **] [dst-ipv6 {** *ipv6-addresss/M* **| ipv6any }] [** *igmp-type] [icmp-type icmp-code* **] [dst-port** *port-number* **] [traffic-class** *traffic-class* **] [time-range** *time-range-name* **];** Command is used to configure the ipv6 hybrid ACL rule

no access-list { all | hybrid-acl-id [subitem-id] }; Ccommand is used to remove the hybrid ACL rules.

【example】

Configuration Hybrid ACL: Discard messages for VLAN 4094, src-mac = 00:00:00:11:11:11 src-ip = 192.168.1.100.

switch#configure terminal

switch(config)#access-list 2000 deny vlan 4094 src-mac 00:00:00:11:11:11 host src-ip 192.168.1.100 host dst-ip any

39.1.6 access-list { mac-acl | ip-acl | hybrid-acl } acl-id

【command】

access-list { mac-acl | ip-acl | hybrid-acl } *acl-id* **[match-order { auto | config }]**

no access-list { all | *mac-acl-id[subitem-id* **] }**

【config-mode】

Global configuration mode

【parameter】

mac-acl：Indicates that by creating a MAC ACL.

ip-acl：Indicates that it is creating a IP ACL.

hybrid-acl：Indicates that by creating a Hybrid ACL.

acl-id：ACL number, integer format, the specific value range is as follows:

IP ACL value range 1-999;

MAC ACL value range 1000-1999;

Hybrid ACL value range 2000-2999.

auto：represents automatic sorting according to depth, deep row and shallow row.

config：using configuration order.

【description】

access-list { mac-acl | ip-acl | hybrid-acl } *acl-id* **[match-order { auto | config }]**; Command is used to create and enter ACL config-mode

no access-list { all | *mac-acl-id [subitem-id* **] }**; Command is used to remove the ACL rules.

【example】

#Configure IP ACL 10, and the matching order is auto.

switch#configure terminal

switch(config)#access-list ip-acl 10 match-order auto

switch(config-ip-nacl-10)#

39.1.7 subitem-id { permit | deny } (MAC-ACL)

【command】

[*subitem-id***] { permit | deny } [** *protocol] { source-mac-addr { mac-wildcard* **| host } | any } {** *destination-mac-addr { mac-wildcard* **| host } | any } [vlan** *vlan-id* **] [cos** *vlan-pri* **] [time-range** *time-range-name* **]**

no *subitem-id*

【config-mode】

MAC ACLconfig-mode

【parameter】

subitem-id：ACL subitem number, integer form, value range from 0 to 127.

permit：indicates forwarding packet matching ACL.

deny：indicates discarding packet matching ACL.

protocol：Agreement number, hexadecimal format, value range: 1 to FFFF.

vlan-pri：VLAN priority, integer form, value range 0~7.

vlan-id：VLAN ID, Integer form, take the value range from 1 to 4094.

source-mac-addr：Source MAC address, format H: H: H: H: H: H.

destination-mac-addr：Purpose MAC address, format H: H: H: H: H: H.

mac-wildcard：The wildcard mask of the source MAC address, format ff: ff: ff: ff: ff: ff.

host：Represents the host address.

time-range：Indicates the effective time domain of the specified ACL rule.

time-range-name：The name of the time domain, in the string format, supports up to 32 characters.

【description】

[*subitem-id*] { **permit | deny** } [*protocol] { source-mac-addr { mac-wildcard* | **host } | any** } { *destination-mac-addr { mac-wildcard* | **host } | any } [vlan** *vlan-id*] [**cos** *vlan-pri*] [**time-range** *time-range-name*] command Use to configure the MAC ACL filtering rules.

no *subitem-idcommand* Use to remove the MAC ACL filtering rules.

【example】

#Configure the MAC ACL 1999, add a subkey: Discards the message for the vlan 4094.

switch#configure terminal

switch(config)#access-list mac-acl 1999

switch(config-mac-nacl-1999)#deny any any 4094

39.1.8 subitem-id { permit | deny } (IP-ACL)

【command】

[*subitem-id* **] { permit | deny } [** *protocol] [icmp-type icmp-code* **] [established] {** *source-ipv4-address { ipv4-mask* **| host } | any } [** *port-number] { destination-ipv4-address { ipv4-mask* **| host } | any } [** *port-number] [igmp-type* **] [precedence** *precedence* **| tos** *tos* **| dscp** *dscp* **| fragments]* [time-range** *time-range-name* **]**

[*subitem-id* **] { permit | deny } [** *protocol] [icmp-type icmp-code* **] [established] {** *source-ipv6/M* **| ipv6any } [** *port-number] { destination-ipv6/M* **| ipv6any } [** *port-number* **] [traffic-class** *traffic-class* **] [time-range** *time-range-name* **]**

no *subitem-id*

【config-mode】

IP ACL config-mode

【parameter】

subitem-id：ACL subitem number, integer format, value range from 0 to 127.

permit：indicates forwarding packet matching ACL.

deny：indicates discarding packet matching ACL.

protocol：Agreement number, support the integer and name format, take the following values:

Integer form, take the value range: 0~255;

name: gre、icmp、icmpv6、igmp、ipinip、ospf、tcp、udp.

source-ipv4-address：Source IPv4 address, point split decimal.

destination-ipv4-address：Objective IPv4 address, points decimal.

ipv4-mask：The IPv4 address mask.

host：Represents the host address.

any：Indicates any IPv4 address.

source-ipv6/M：Source IPv6 address and mask length.

destination-ipv6/M：Purpose IPv6 address and mask length.

ipv6any：Indicates any IPv6 address.

icmp-type icmp-code：icmp Type and subtypes, only available with protocol icmp, icmpv6, integer and name format supported with the following values:

Integer form: value range 0-255;

name：echo、echo-reply、fragmentneed-dfset、host-redirect、 host-tos-redirect、host-unreachable、information-reply、 information-request、net-redirect、net-tos-redirect、net-unreachable、 parameter-problem、port-unreachable、protocol-unreachable、reassembly-timeout、source-quench、source-route-failed、timestamp-reply、timestamp-request、ttl-exceeded；

established：Indicates SYN = 1 in TCP and is only available when the protocol is TCP.

port-number：Transport layer port number, integer form, supports three formats:

Decimal: value range 1- 65535;

Octal: value range 0-0177777, input starts with 0, automatically converted to decimal when distribution configuration;

Headecimal:value range 0-0xffff, input starts with 0x, automatically converted to decimal when distribution configuration;

wildcard：Transport layer port number wildcard mask.

igmp-type：IGMP protocol type, only available when the protocol is IGMP, integer format, value range 0-34.

precedence：IP priority, support for integer and name format, specific as follows:

Integer format: value range 0-7;

name: routine、priority、immediate、flash、flash-override、critical、internet、 network.

tos：ToS priority, support integer and name format, with the following values:

Integer format: the value range is from 0 to 15;

Name: max-reliability (value 2), max-throughput (value 4), min-delay (value 8), min-monetary-co (value 1), normal (value 0).

dscp：DSCP priority, support for integer and name format, specifically as follows:

Integer format: the value range is from 0 to 63;

Name: af1(10)、af2(18)、af3(26)、af4(34)、cs1(8)、cs2(16)、cs3(24)、cs4（32）、cs5（40）、 cs6(48)、cs7(56)、be(0)、ef(46);

fragments：do not fragmentation: DF=1.

traffic-class：IPv6 priority, integer format, value range 0 to 63.

time-range-name：time range name, string format, supports up to 32 characters.

【description】

[*subitem-id*] { **permit | deny** } [*protocol] [icmp-type icmp-code*] [**established**] { *source-ipv4-address { ipv4-mask* | **host } | any** } [*port-number] { destination-ipv4-address { ipv4-mask* | **host } | any** } [*port-number] [igmp-type*] [**precedence** *precedence* | **tos** *tos* | **dscp** *dscp* | **fragments]* [time-range** *time-range-name*]; Command is used to configure the IPv4 ACL filtering rules.

[*subitem-id*] { **permit | deny** } [*protocol] [icmp-type icmp-code*] [**established**] { *source-ipv6/M* | **ipv6any** } [*port-number] { destination-ipv6/M* | **ipv6any** } [*port-number*] [**traffic-class** *traffic-class*] [**time-range** *time-range-name*]; Command is used to configure the IPv6 ACL filtering rules.

no *subitem-id*; Command is used to remove the ACL subitem.

【example】

#Configuration IP ACL 10: Discards the ICMP messages.

switch#configure terminal

switch(config)#access-list ip-acl 10

switch(config-ip-nacl-10)#deny icmp any any

39.1.9 subitem-id { permit | deny } (Hybrid-ACL)

【command】

[*subitem-id* **] { permit | deny } [** *ip-protocol* **] [vlan** *vlan-id* **] [cos** *vlan-pri* **][src-mac** *src-mac-addr { mac-wildcard* **| host }] [dst-mac** *dst-mac-addr { mac-wildcard* **| host }] [src-ip** *ip-address { ip-mask* **| any }] [src-port** *port-number* **] [dst-ip** *ip-address { ip-mask* **| any }] [** *igmp-type] [icmp-type icmp-code* **] [dst-port** *port-number* **] [precedence** *precedence* **| tos** *tos* **| dscp** *dscp* **| fragments]*[time-range** *time-range-name* **]**

[*subitem-id* **] { permit | deny } [** *ip-protocol* **] [vlan** *vlan-id* **] [cos** *vlan-pri* **][src-mac** *src-mac-addr { mac-wildcard* **| host }] [dst-mac** *dst-mac-addr { mac-wildcard* **| host }] [src-ipv6 {** *ipv6-addresss/M* **| ipv6any }] [src-port** *port-number* **] [dst-ipv6 {** *ipv6-addresss/M* **| ipv6any }] [** *igmp-type] [icmp-type icmp-code* **] [dst-port** *port-number* **] [traffic-class** *traffic-class* **] [time-range** *time-range-name* **]**

no *subitem-id*

【config-mode】

Hybrid ACL config-mode

【parameter】

subitem-id：ACL subitem number, integer format, value range 0-127.

permit：indicates forwarding packet matching ACL.

deny：indicates discarding packet matching ACL.

ip-protocol：Agreement number, integer format, value range 0-255.

vlan-pri：VLAN priority, integer format, value range 0-7.

vlan-id：VLAN ID, integer format, value range 1-4094.

src-mac-addr：Source MAC address, format H: H: H: H: H: H.

dst-mac-addr：destination MAC address, format H: H: H: H: H: H.

mac-wildcard：MAC address wildcard mask, format ff: ff: ff: ff: ff: ff.

host：Represents the host address.

ip-address：IPv4 address, points in the decimal system.

ip-mask：The IPv4 address mask.

any：Indicates any IPv4 address.

ipv6any：Indicates any IPv6 address.

ipv6-address/M：IPv6 address and mask length.

icmp-type icmp-code：The icmp type and subtype, integer format, value range 0-255.

established：Indicates SYN = 1 in TCP and is only available when the protocol is TCP.

port-number：Transport layer port number, integer form, supports three formats:

Decimal: value range from 1 to 65535;

Octal: value range 0-0177777, input starts with 0, automatically converted to decimal when distribution configuration;

Headecimal:value range 0-0xffff, input starts with 0x, automatically converted to decimal when issuing configuration;

wildcard：Transport layer port number wildcard mask.

igmp-type：IGMP protocol type, only available when the protocol is IGMP, integer format, value range 0-34.

precedence：IP priority, integer format, value range from 0-7.

tos：ToS priority, integer format, value range 0-15.

dscp：DSCP priority, integer format, value range 0-63.

fragments：do not fragmentation: DF=1.

traffic-class：IPv6 priority, integer format, value range 0-63.

time-range-name：time range name, string format, supports up to 32 characters.

【description】

subitem-id { **permit | deny** }; Command is used to configure hybrid ACL subitem.

no *subitem-id*; Command is used to remove hybrid ACL subitem.

【example】

#Configuration Hybrid ACL: Discard the VLAN 4094 source IP=1.1.1.1/32

switch#configure terminal

switch(config)#access-list hybrid-acl 2000

switch(config-hybrid-nacl-2000)#deny vlan 4094 src-ip 1.1.1.1 host dst-ip any

39.1.10 access-group

【command】

access-group ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] { in | out }**

access-group mac-acl *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] { in | out }**

access-group hybrid-acl *hybrid-acl-id* **subitem** *subitem-id* **{ in | out }**

no access-group { all | { hybrid-acl *hybrid-acl-id* **[subitem** *subitem-id* **] } } { in | out }**

no access-group ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] { in | out }**

no access-group mac-acl *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id***]] { in | out }**

【config-mode】

Global \ port \ Lacp config-mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

【description】

access-group; Command is used to activate the ACL.

no access-group; Command is used to unactivate the ACL.

By default, no ACL is activated.

【example】

#Activate the IP ACL 1 in the global mode.

switch#configure terminal

switch(config)#access-group ip-acl 1 in

39.1.11 time-range

【command】

time-range *time-range-name*

no time-range *time-range-name*

【config-mode】

any config-modes except the execution and privileged config-mode

【parameter】

time-range-name：Time range name, support up to 32 characters, must start with an English letter, not case-sensitive.

【description】

time-range *time-range-name*; Command is used to configure the time range and entering the time-range config-mode;

no time-range *time-range-name*; Command is used to delete the time range configuration.

By default, there is no any time-range configuration.

【example】

#Create the time range:name abc.

switch(config)#time-range abc

switch(config-timerange-abc)#

39.1.12 absolute

【command】

absolute [start *hh:mm:ss yyyy/mm/dd* **[end** *hh:mm:ss yyyy/mm/dd* **]]**

no absolute [start *hh:mm:ss yyyy/mm/dd* **[end** *hh:mm:ss yyyy/mm/dd* **]]**

【config-mode】

time-range config-mode

【parameter】

start：Represents the start time of the time range.

hh:mm:ss yyyy：Hours, minutes, and seconds for a fixed time period.

hh: hours,value range 0-23.

mm: minutes,value range 0-59.

ss: second,value range 0-59.

yyyy/mm/dd：Date of the specified period: year, month, and date;

dd: date, value range from 1-31.

mm:month, value range 1-12.

yy: year,value range 2000-2099.

end：Represents the end time.

【description】

absolute [**start** *hh:mm:ss yyyy/mm/dd* [**end** *hh:mm:ss yyyy/mm/dd*]];Command is used to configure the absolute time period.

no absolute [**start** *hh:mm:ss yyyy/mm/dd* [**end** *hh:mm:ss yyyy/mm/dd*]];Command is used to remove the absolute time period.

Time domain is a collection of time periods. A time range domain can contain zero to multiple time periods. The time range is the union of each time period.

【example】

#Configuration absolute time period: starting time: 2020 / 1 / 1 8:00 End time: 2020 / 1 / 10 8:00

switch#configure terminal

switch(config)#time-range range-name

switch(config-timerange-range-name)#absolute start 00:08:00 2020/1/1 end 00:08:00 2020/1/10

39.1.13 periodic

【command】

periodic *days-of-week hh:mm:ss* **to** *hh:mm:ss*

no periodic *days-of-week hh:mm:ss* **to** *hh:mm:ss*

【config-mode】

time-range config-mode

【parameter】

days-of-week: The specified cycle period takes effect on the day of the week and can be entered multiple times, but the later entered value cannot completely overlap with the previously entered value. Integers and names are supported, specifically as follows:

Integer: value range 0-6,0 indicates Sunday.

Name :fri、mon、sat、sun、thu、tue、wed、weekdays、weekend。

yyyy/mm/dd: Date of the specified period: year, month, and date;

dd: Date,value range 1-31.

mm: month, value range 1-12.

yy: Year,value range 2000-2099.

【description】

periodic *days-of-week hh:mm:ss* **to** *hh:mm:ss*; Command is used to configure the time rage period.

no periodic *days-of-week hh:mm:ss* **to** *hh:mm:ss*;Command is used to remove the time range priod.

【example】

#Configure periodic periods: 8:00 to 12:00 every Monday.

switch#configure terminal

switch(config)#time-range range-name

switch(config-timerange-range-name)#periodic 1 08:00:00 to 12:00:00

39.2 ACL Monitoring and debugging command

39.2.1 show time-range

【command】

show time-range { all | name *time-range-name* **| statistic }**

【config-mode】

Global configuration mode

【parameter】

All: Represents all of the time-range configurations

time-range-name: time range name, string format, support up to 32 characters.

statistic: Represents to view the time-range statistics.

【description】

show time-range { all | name *time-range-name* | **statistic }**; Command is used to view the time-domain configuration information.

【example】

#View the time range "named" configuration information

switch#show time-range name range-name

Current time is: 14:52:15 2013/01/01 Tuesday

time-range: range-name (Inactive)

periodic: sun 08:00:00 to 12:00:00

39.2.2 show access-list config

【command】

show access-list config { all | *acl-id* **| brief }**

【config-mode】

Global configuration mode

【parameter】

all: ACL number, integer format, value range 1-2999.

brief：Represents viewing the ACL brief information.

【description】

show access-list config { all | *acl-id* **| brief }**; Command is used to view ACL information.

【example】

#View the ACL configuration information.

switch#show access-list config all

IP Access List 1, match-order is config, 0 rule:

Mac Access List 1000, match-order is config, 0 rule:

Hybrid Access List 2000, match-order is config, 2 rule:

0 : deny vlan 4094 src-mac 00:00:00:11:11:11 ff:ff:ff:ff:ff:ff src-ip 192.1

68.1.100 255.255.255.255 dst-ip any

5 : permit vlan 4094 src-ip any dst-ip any

total config rules: 2 rules

39.2.3 show access-list runtime

【command】

show access-list runtime { all | *acl-id* **| brief }**

【config-mode】

Global configuration mode

【parameter】

all: all ACL configurations.

acl-id: ACL number, integer format, value range 1-2999.

brief: Represents viewing the ACL brief information.

【description】

show access-list runtime { all | *acl-num* **| brief }**; Command is used to view the activated ACL configuration information.

【example】

#View the ACL activation configuration information.

switch#show access-list runtime all

access-list 2000 subitem 0 running inbound

access-list 2000 subitem 5 running inbound

total runtime rules: 2 rules

Chapter 40 QACL

40.1 QACL configure command

40.1.1 traffic priority

【command】

traffic priority { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *hybrid-acl-id* **[subitem** *subitem-id* **] } { [cos** *vlan-pri* **| local-precedence** *local-precedence* **] | [dscp** *dscp* **| precedence** *precedence* **] }***

no traffic priority { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *hybrid-acl-id* **[subitem** *subitem-id* **] }**

【config-mode】

Global \ port config-mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

vlan-pri：VLAN priority, support for integer and string format, specifically as follows:

Integer form, take the value range from 0 to 7.

Name: background(0)、best-effort(2)、controlled-load(4)、excellent-effort(3)、network-management (7)、spare (1)、video (5)、voice (6).

local-precedence：Local priority, integer format, and value range is from 0 to 7.

dscp：DSCP Priority, support for integer and name format, specific as follows:

Integer: value range is 0 to 63;

Name: af1(10)、af2(18)、af3(26)、af4(34)、cs1(8)、cs2(16)、cs3(24)、cs4(32)、cs5(40)、cs6(48)、cs7(56)、be(0)、ef(46);

precedence：IP priority, support integer and name format, specific as follows:

Integer:value range is 0 to 7;

Name:routine,priority, immediate, flash, flash-override, critical, internet or network.

【description】

traffic priority; Command is used to modify the priority of the specified flow.

no traffic priority; Command is used to delete the configuration.

By default, the function for the flow to modify the priority is not configured.

【example】

#Modify the stream VLAN priority for matching IP ACL1 to 7.

switch#configure terminal

switch(config)#traffic priority ip-acl 1 cos 7

40.1.2 traffic insert-vlan

【command】

traffic insert-vlan { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] }** *vlan-id*

no traffic insert-vlan { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] }**

【config-mode】

Global \ port config-mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

vlan-id：VLAN ID，Integer format, value range 1-4094.

【description】

traffic insert-vlan; Command is used to configure insert-vlan in the specified stream.

no traffic insert-vlan; Command is used to delete configuration.

By default, the flow-insert VLAN feature is not configured.

【example】

#Configure the flow matching the IP ACL 1 to insert VLAN 4094.

switch#configure terminal

switch(config)#traffic insert-vlan ip-acl 1 4094

40.1.3 traffic rewrite-vlan

【command】

traffic rewrite-vlan { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] }** *vlan-id*

no traffic rewrite-vlan { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] }**

【config-mode】

Global \ port config-mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

vlan-id：VLAN ID, Integer format, take the value range from 1 to 4094.

【description】

traffic rewrite-vlan; Command is used to modify VLAN matching ACL.

no traffic rewrite-vlan; Command is used to delete configuration.

Must be a permit ACL. The vlan-id must exist and contain the port.

By default, there is no traffic rewrite-vlan configuration.

【example】

#Change the flow VLAN for matching IP ACL 1 to 4000.

switch#configure terminal

switch(config)#traffic rewrite-vlan ip-acl 1 4000

40.1.4 traffic redirect

【command】

traffic redirect { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] } { interface ethernet** *port-id* **| CPU }**

no traffic redirect { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] }**

【config-mode】

Global \ port config-mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

port-id：Port number, value range is determined by the system hardware, and the format is 0/0/1.

CPU：Represents the CPU port.

【description】

traffic insert-vlan; Command is used to configure the flow redirection to the specified port.

no traffic insert-vlan; Command is used to restore the default configuration.

Redirection means that the message is not forwarded according to the original destination address, but is redirected to the specified exit port.

Notes: if redirected to the CPU, which may affect performance.

By default, flow redirection is not configured.

【example】

#Configure the flow redirection of the matching IP ACL 1 to the port 0/0/1.

switch#configure terminal

switch(config)#traffic redirect ip-acl 1 interface ethernet 0/0/1

40.1.5 traffic statistic

【command】

traffic statistic { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] } { in | out }**

no traffic statistic { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] } { in | out }**

【config-mode】

Global\Port config-mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

in：mean working input direction.

out：mean working output direction.

【description】

traffic statistic; Command is used to configure the statistical specified flow.

no traffic statistic; Command is used to restore the default situation.

You must first configure the ACL to use the command.

By default, the flow statistics is not configured.

【example】

#Statistics were performed on the incoming orientation data of flow IP ACL 1.

switch#configure terminal

switch(config)#traffic statistic ip-acl 1 in

40.1.6 traffic mirror

【command】

traffic mirror { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] } interface ethernet** *port-id*

no traffic mirror { ip-acl *ip-acl-id* **[subitem** *subitem-id* **] [mac-acl** *mac-acl-id* **[subitem** *subitem-id* **]] | mac-acl** *mac-acl-id* **[subitem** *subitem-id* **] [ip-acl** *ip-acl-id* **[subitem** *subitem-id* **]] | hybrid-acl** *acl-id* **[subitem** *subitem-id* **] }**

【config-mode】

Global configuration mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

port-id：Port number, value range is determined by the system hardware, and the format is 0/0/1.

【description】

traffic mirror; Command is used to configure the specified stream to mirror port.

no traffic mirror; Command is used to restore the default situation.

The default, the flow mirror function is not configured.

【example】

#Configuring mirror matches the 0/0/1 flow to port of ip-acl 1.

switch#configure terminal

switch(config)#traffic mirror ip-acl 1 interface ethernet 0/0/1

40.1.7 traffic rate-limit

【command】

traffic rate-limit { **ip-acl** *ip-acl-id* [**subitem** *subitem-id*] [**mac-acl** *mac-acl-id* [**subitem** *subitem-id*]] | **mac-acl** *mac-acl-id* [**subitem** *subitem-id*] [**ip-acl** *ip-acl-id* [**subitem** *subitem-id*]] | **hybrid-acl** *acl-id* [**subitem** *subitem-id*] } *rate* { **in** | **out** }

no traffic rate-limit { **ip-acl** *ip-acl-id* [**subitem** *subitem-id*] [**mac-acl** *mac-acl-id* [**subitem** *subitem-id*]] | **mac-acl** *mac-acl-id* [**subitem** *subitem-id*] [**ip-acl** *ip-acl-id* [**subitem** *subitem-id*]] | **hybrid-acl** *acl-id* [**subitem** *subitem-id*] } { **in** | **out** }

【config-mode】

Global \ port config-mode

【parameter】

ip-acl-id：IP ACL Number, integer format, value range 1-999.

mac-acl-id：MAC ACL Number, integer format, value range 1000-1999.

hybrid-acl-id：Hybrid ACL Number, integer format, value range 2000-2999.

subitem-id：ACL subitem number, integer format, value range 0-127.

rate：Speed limit value, integer format, value range 64-maximum rate, unit Kbps.

in：Represents the inputting speed limit.

out：Represents the outputting directional speed limit.

【description】

traffic rate-limit; Command Is used to configure the specified flow speed limit.

no traffic rate-limit; Command is used to restore the default configuration.

In default, there is no configuration.

Successful configuration is a multiple of 64, downward compatibility, such as input command is 65, successful configuration will automatically become 64.

【example】

#The configuration speed limits 6400 Kbps for the flow in direction of matching ip-acl 1.

switch#configure terminal

switch(config)#traffic rate-limit ip-acl 1 6400 in

40.2 QACL Monitoring and debugging command

40.2.1 show traffic

【command】

show traffic { all | insert-vlan | priority | redirect | rewrite-vlan | statistic | mirror | brief }

【config-mode】

Any config-mode

【parameter】

None

【description】

show traffic; Command is used to view all the flow configuration information.

【example】

#View all of the configuration information.

switch#show traffic all

Traffic-mirror:

rate-limit:

Traffic-priority:

Traffic-redirect:

Traffic-statistic:

Traffic-rewrite-vlan:

Traffic-insert-vlan:

show traffic information description

field	instruction
Traffic-mirror	Flow mirror configuration
rate-limit	Flow speed limit configuration
Traffic-priority	Modify the priority configuration
Traffic-redirect	Redirect configuration
Traffi- rewrite-vlan	Modify the VLAN configuration
Traffic-insert-vlan	Insert the VLAN configuration

Chapter 41 Two-speed three-color

41.1 Two-speed three-color configuration command

41.1.1 two-rate-policer mode

【command】

two-rate-policer mode { color-aware | color-blind }

no two-rate-policer mode

【config-mode】

Global configuration mode

【parameter】

color-aware: specifies the color-sensitive mode. In this mode, the traffic supervision action to consider the original color of the message.

color-blind: specifies the color-blind mode. In this mode, the original color of the message does not affect the flow of the traffic supervision action.

【description】

two-rate-policer mode { color-aware | color-blind }; Command is used to configure the two-speed three-color mode.

no two-rate-policer mode; Command is used to restore the default configuration.

By default, the two-speed three-color mode is color-bold.

【example】

#Configure two-speed three-color mode for color-blind。

switch#configure terminal

switch(config)#two-rate-policer mode color-blind

41.1.2 two-rate-policer set-pre-color

【command】

two-rate-policer set-pre-color *dscp_value* **{ green | yellow | red }**

no two-rate-policer set-pre-color [*dscp_value* **]**

【config-mode】

Global configuration mode

【parameter】

dscp_value：DSCP Value, integer format, value range from 0 to 63.

【description】

two-rate-policer set-pre-color *dscp_value* **{ green | yellow | red }**; Command is used to configure the color labeling for the different DSCP values.

no two-rate-policer set-pre-color [*dscp_value* **]**; Command is used to restore default configuration.

By default, all DSCP values are colored as green.

【example】

#mark message with DSCP value 3 green.

switch#configure terminal

switch(config)#two-rate-policer set-pre-color 3 green

41.1.3 two-rate-policer policer-id

【command】

two-rate-policer *policer-id* **cir** *cir-value* **[cbs** *cbs-value***] pir** *pir-value* **[pbs** *pbs-value* **] [green-action { copy-to-cpu | drop | set_dscp_value** *dscp_value* **| transmit } yellow-action { copy-to-cpu | drop | set_dscp_value** *dscp_value* **| transmit } red-action { copy-to-cpu | drop | set_dscp_value** *dscp_value* **| transmit }]**

no two-rate-policer *policer-id*

【config-mode】

Global configuration mode

【parameter】

policer-id：Policy ID value, integer format, value range from 0 to 255.

cir：Represents the promised information rate.

cir-value：The cir rate value, integer format, value range 64-10000000,unit kbps.

cbs：Indicates the cir burst size.

cbs-value：The cbs rate value, integer format, 3600-1073741824, unit byte.

pir：Represents the peak information rate.

pir-value：The pir rate value, integer format, ranges from 64-10000000,unit kbps.

pbs：Indicates the pir burst size.

pbs-value：The pbs rate value, integer format, 3600-1073741824, unit byte.

green-action：Represents the processing behavior of the green messages.

yellow-action：Represents the processing behavior of the yellow messages.

red-action：Represents the processing behavior of the red messages.

copy-to-cpu：Indicates the processing behavior of copying to the CPU port.

drop：Indicates the processing behavior of discarding.

set_dscp_value：Indicates the processing behavior as setting the DSCP value.

transmit：It means that the processing behavior is a forwarded message.

dscp_value：DSCP value, integer format, value range from 0 to 63.

【description】

two-rate-policer *policer-id*; Command is used to configure two-speed three-color strategy.

no two-rate-policer *policer-id*; Command is used to remove the configured policy.

【example】

#Configure two-speed three color strategy 1

switch#configure terminal

switch(config)#two-rate-policer 1 cir 10000 pir 20000 pbs 100000 green-action drop yellow-action transmit red-action drop

41.1.4 traffic rate-limit acl-id two-rate-policer

【command】

traffic rate-limit { hybrid-acl | ip-acl | mac-acl } *acl-id* **two-rate-policer** *policer-id* **in**

no traffic rate-limit *acl-id* **in**

【config-mode】

Global configuration mode

【parameter】

acl-id：ACL number, integer format, value range 1-2999.

policer-id：Policy ID value, integer format, value range 0-255.

in：Represents that the input direction is effective.

【description】

traffic rate-limit { hybrid-acl | ip-acl | mac-acl } *acl-id* **two-rate-policer** *policer-id* **in**; Command is used to enable the two-speed three-color strategy function.

no no traffic rate-limit *acl-id* **in**; Command is used to delete the configuration.

The applied two-speed three-color strategy must be configured first, or the command will fail.

【example】

#The two-speed three olor strategy 0 was applied to the IP acl 1 entry flow

switch#configure terminal

switch(config)#access-list 1 permit 1.1.1.1 host any

switch(config)#two-rate-policer 1 cir 10000 pir 20000 pbs 100000 green-action drop yellow-action transmit red-action drop

switch(config)#traffic rate-limit ip-acl 1 two-rate-policer 0 in

41.2 Two-speed three-color monitoring and debugging command

41.2.1 show two-rate-policer [policer-id]

【command】

show two-rate-policer [*policer-id* **]**

【config-mode】

Global configuration mode

【parameter】

policer-id：Policy ID value, integer format, value range from 0 to 255.

【description】

show two-rate-policer; Command is used to view the two-speed three-color configuration.

【example】

#View the two-speed three-color policy configuration.

switch(config)#show two-rate-policer

two rate policer 1 :

CIR : 10000Kbps CBS : 10000bytes PIR : 10000Kbps PBS : 100000bytes

color aware : color-aware

green action: copy-to-cpu

yellow action: transmit

red action: drop

reference count : 0

show two-rate-policerdisplay field description

field	instruction
two rate policer 1	policy id

field	instruction
CIR	CIR configuration value
CBS	CBS configuration value
PIR	PIR Configuration value
PBS	PBS Configuration value
color aware	Color mode
green action	Handling behavior of green messages
yellow action	Handling behavior of yellow messages
red action	Handling behavior of red messages
reference count	Match times

41.2.2 show two-rate-policer

【command】

show two-rate-policer set-pre-color

【config-mode】

Global configuration mode

【parameter】

None

【description】

show two-rate-policer set-pre-color; Command is used to view the two-speed three-color configuration details.

【example】

#Check out the two-speed three-color configuration details.

switch(config)#show two-rate-policer set-pre-color

queue-scheduler dscp-map is open.

trTCM mode is color-aware.

Information about map of dscp to pre-color:

DSCP value marked pre-color

---

0 green

1 green

2 green

3 green

4 green

5 green

6 green

7 green

8 green

……

60 green

61 green

62 green

63 green

show two-rate-policer display field description

field	instruction
DSCP value	dscp price
marked pre-color	The color of the mark

Chapter 42 bandwidth control

42.1 Bandwidth control configuration command

42.1.1 bandwidth ingress

【command】

bandwidth ingress { kbps *rate-value* **| percent** *percent-value* **}**

no bandwidth ingress

【config-mode】

Port config-mode

【parameter】

ingress：means working on input direction.

kbps：means unit Kbps.

rate-value：speed value, integer format, value range 16-10000000,unit kbps.

percent：means unit %.

percent-value：speed value, integer format, value range 1-99, unit %.

【description】

bandwidth ingress { kbps *rate-value* **| percent** *percent-value* **}**; Command is used to configure the input direction bandwidth speed limit.

no bandwidth ingress commandUsed to restore the default configuration.

By default, no speed limit is configured, work at maximum port rate.

【example】

#set port 0/0/1 ingress speed is 100M

switch#configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#bandwidth ingress kbps 100000

42.1.2 bandwidth egress

【command】

bandwidth egress { kbps *rate-value* **| percent** *percent-value* **}**

no bandwidth egress

【config-mode】

Port of the config-mode

【parameter】

egress：means working outgoing directional speed limit.

kbps：means unit Kbps.

rate-value：speed value, integer format, value range 16-10000000,unit kbps.

percent：means unit %.

percent-value：speed value, integer format, value range 1-99, unit %.

【description】

bandwidth egress { kbps *rate-value* **| percent** *percent-value* **};** Command is used to configure the egress directional bandwidth speed limit.

no bandwidth egress; Command is used to restore the default configuration.

By default, there is no bandwidth speed limit ,work at the maximum port rate.

【example】

#Configure port 0/01 egress bandwidth 100M.

switch#configure terminal

switch(config)#interface ethernet 0/0/1

switch(config-if-ethernet-0/0/1)#bandwidth egress 100000

42.1.3 bandwidth queue

【command】

bandwidth queue *queue-id* **limit** *limit-value*

no bandwidth queue *queue-id*

【config-mode】

Port config-mode

【parameter】

queue-id：Port queue ID, integer format, value range 0-7.

limit-value：speed value, integer format, value range 16-10000000,unit kbps.

【description】

bandwidth queue *queue-id* **limit** *limit-value*; Command is used to set CPU speed limit in special queue.

no bandwidth queue *queue-id*; Command is used to restore the default configuration.

By default, it is disable of queue bandwidth limit.

【example】

Configure port 0/0/1 queue 1 limit 16 kbps

switch#configure terminal

switch(config-if-ethernet-0/0/1)#bandwidth queue 1 limit 16

42.2 Bandwidth control, monitoring and debugging command

42.2.1 show bandwidth interface

【command】

show bandwidth interface [ethernet *port-id* **]**

【config-mode】

Global configuration mode

【parameter】

port-id: Port number, value range is determined by system hardware, and format such as 0/0/1.

【description】

show bandwidth interface [ethernet *port-id* **]**; Command is used to display configuration.

【example】

#View the port 0 / 0 / 1 bandwidth speed limit configuration.

switch#show bandwidth interface ethernet 0/0/1

Port-bandwidth informations:

port ingress bandwidth egress bandwidth

e0/0/1 100000kbps 100000kbps

show bandwidth interface ethernet 0/0/1display field description

field	instruction
port	port number
ingress bandwidth	Input direction
egress bandwidth	Output direction

42.2.2 show bandwidth queue interface

【command】

show bandwidth queue interface [ethernet *port-id* **]**

【config-mode】

Global configuration mode

【parameter】

port-id：Port number, the value range is determined by system hardware, and format such as 0/0/1.

【description】

show bandwidth queue interface [ethernet *port-id* **]**; Command is used to view the port queue speed limit configuration

【example】

#View the queue speed limit configuration for port e 0/0/1

switch(config-if-ethernet-0/0/1)#show bandwidth queue interface ethernet 0/0/1

port queue informations:

port: e0/0/1

queue of class queue bandwidth limit

0 disable

1 10000 kbps

2 disable

3 disable

4 disable

5 disable

6 disable

7 disable

show bandwidth queue interface ethernet 0/0/1dislay field description

field	instruction
port	port number
ingress bandwidth	Input direction
egress bandwidth	Output direction

Chapter 43 Storm-control

43.1 Storm-control configuration commands

43.1.1 storm-control action

【command】

storm-control action { logging | shutdown | trap }

no storm-control action

【config-mode】

port configuration mode

【parameter】

action logging: Indicates logging when a packet greater than the configured threshold is received.

action shutdown: Indicates a shutdown port when a packet larger than the configured threshold is received.

action trap: Indicates that a trap alarm is sent when a packet is received that is larger than the configured threshold.

【description】

storm-control action Command is used to configure the handling behavior in case of an attack.

no storm-control action Command is used to remove the processing behavior when under attack, to restore the default behavior: only discard packets that exceed the threshold value.

The action configuration will clear other storm-control-related configurations, so make sure the action command is configured first.

Action shutdown takes effect only when errdisable is enabled. errdisable is enabled by default.

Action trap must be configured with snmp-server related commands to take effect.

【example】

#Configure the handling behavior of port 0/0/1 to logging when it is under storm attack.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)##storm-control action logging

43.1.2 storm-control { broadcast | multicast | unicast }

【command】

storm-control { broadcast | multicast | unicast } [kbps *kbps-value* **| pps** *pps-value* **]**

no storm-control { broadcast | multicast | unicast }

【config-mode】

port configuration mode

【parameter】

broadcast: Indicates configuration of broadcast storm control.

multicast: Indicates configuration of multicast storm control.

unicast: Indicates that unknown unicast storm control is configured.

kbps *kbps-value*: Indicates that the byte-based suppression threshold is configured, ranging from 16 to 1000000, and must be a multiple of 16, unit kbps.

pps *pps-value*: Indicates the configuration of the suppression threshold based on the number of packets, the value range is 1-14881000, in pps.

【description】

storm-control{ broadcast | multicast | unicast } Command to enable storm control and configure suppression threshold.

no storm-control{ broadcast | multicast | unicast } Command to disable storm control while removing suppression thresholds.

Storm control is disabled by default.

【example】

#Limit the maximum forwarding rate of unknown unicast packets to 100kpps on port e0/0/1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#storm-control unicast kbps 100

43.2 Storm-control monitoring commands

43.2.1 show storm-control interface

【command】

show storm-control interface [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, configuration range determined by switch hardware model.

【description】

show storm-control interface Command displays the storm control configuration information of the port.

【example】

#View storm control packet types and suppression thresholds

Switch(config)#show storm-control

Port number: e0/0/1

storm-control action: trap

Broadcast storm control target rate is 100pps

Multicast storm control has been disabled

Unicast storm control has been disabled

Total entries: 1.

storm-control display field description

Field	Description

Port number	Port number
storm-control action	Attack handling behavior: NA、logging、shudown、trap
Broadcast storm control target rate is 100pps	Broadcast Storm Control Suppression Rate Threshold
Multicast storm control has been disabled	Multicast storm control enable status: disabled, specific threshold
Unicast storm control has been disabled	Unicast storm control enable status: disabled, specific threshold
Total entries	Statistical Information

Chapter 44 ARP anti-spoofing

44.1 ARP anti-spoofing configuration commands

44.1.1 arp anti-spoofing

【command】

arp anti-spoofing

no arp anti-spoofing

【config-mode】

Global configuration mode

【parameter】

None

【description】

arp anti-spoofing Command to enable protection against ARP spoofing attacks.

no arp anti-spoofing Command to disable protection against ARP spoofing attacks.

The default is disable, and when enabled, the default action drops all ARP packets. Before enable arp anti-spoofing, it is suggested to configure static ARP for management PC on the device, otherwise it will cause management interruption after enable.

【example】

#Enabling ARP Spoofing.

Switch#configure terminal

Switch(config)#arp anti-spoofing

44.1.2 arp anti-spoofing action

【command】

arp anti-spoofing action { discard | flood }

【config-mode】

Global configuration mode

【parameter】

discard: The processing action for unknown arp is discard.

flood: Flooding for unknown arp processing action.

【description】

arp anti-spoofing action Command is used to configure the processing action for unknown arp.

By default, the processing action for unknown arp is discard.

【example】

#Configure action as flooding.

Switch#configure terminal

Switch(config)#arp anti-spoofing action flood

44.1.3 arp anti-spoofing bind

【command】

arp anti-spoofing bind ip *ip-value* **interface [ethernet** *port-id* **]**

no arp anti-spoofing bind ip *ip-value* **interface [ethernet** *port-id* **]**

【config-mode】

Global configuration mode

【parameter】

ip-value: Host protection function binds the ipv4 address.

port-id: The port number to which the host protection function is bound, the configuration range is determined by the hardware model.

【description】

arp anti-spoofing bind Command is used to configure the host protection table entry. If arp anti-spoofing is enabled, the system will forward the ARP packets matching the host protection table entry.

no arp anti-spoofing bind Command to delete user host protection table entries.

【example】

#Configure ip address 1.1.1.1 and port e0/0/1 binding.

Switch#configure terminal

Switch(config)#arp anti-spoofing bind 1.1.1.1 ethernet 0/0/1

44.1.4 arp anti-spoofing gateway-disguiser

【command】

arp anti-spoofing gateway-disguiser

no arp anti-spoofing gateway-disguiser

【config-mode】

Global configuration mode

【parameter】

None

【description】

arp anti-spoofing gateway-disguiser Command is used to enable the gateway anti-spoofing function. When enabled, the system will send the gateway impersonator down to the black hole table entry, and at the same time send the correct ARP.

no arp anti-spoofing gateway-disguiser Command to disable the gateway's anti-spoofing feature.

Default disable.

【example】

#Enables gateway anti-spoofing feature.

Switch#configure terminal

Switch(config)#arp anti-spoofing

Switch(config)#arp anti-spoofing gateway-disguiser

44.1.5 arp anti-spoofing source-mac-check

【command】

arp anti-spoofing source-mac-check

no arp anti-spoofing source-mac-check

【config-mode】

Global configuration mode

【parameter】

None

【description】

arp anti-spoofing source-mac-check Command enables the source address consistency check function for arp messages. After enabling the function, the system will discard ARP packets with inconsistent source MAC in the Ethernet frame and the source MAC in the ARP header.

no arp anti-spoofing source-mac-check The command disables the source address consistency check function of arp packets.

Default disable.

【example】

#Enable arp packet source address consistency check.

Switch#configure terminal

Switch(config)#arp anti-spoofing

Switch(config)#arp anti-spoofing source-mac-check

44.1.6 arp anti-attack trust

【command】

arp anti-attack trust

no arp anti-attack trust

【config-mode】

Port Configuration Mode

【parameter】

None.

【description】

arp anti-attack trust Command is used to enable the port as a trusted port.

no arp anti-attack trust Command is used to disable the trusted port.

After enabling the trust port, the received ARP packets are forwarded without attack and spoofing checks.

Default is untrust.

【example】

#Enable port ethernet 0/0/1 as trust port.

Switch#configure terminal

Switch(config-if-ethernet-0/0/1)#arp anti-attack trust

44.2 ARP anti-spoofing monitoring commands

44.2.1 show arp anti-spoofing

【command】

show arp anti-spoofing

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show arp anti-spoofing Command to view arp anti-spoofing configuration information.

【example】

#View ARP anti-spoofing information.

Switch(config-if-ethernet-0/0/1)#show arp anti-spoofing

Informations of arp anti-spoofing

ARP anti-spoofing status: Disabled

ARP anti-spoofing entry: 0

ARP anti-spoofing unknown-packet policy: Discard

anti-spoofing gateway-disguiser: Enabled

arp anti-spoofing source-mac-check: Enabled

arp anti-spoofing display field description.

Field	Description
ARP anti-spoofing status	ARP anti-spoofing function enable state
ARP Anti-Spoofing entry	Number of protected host table entries
ARP anti-spoofing unknown-packet policy	Processing action for unknown ARP packets: discard、flood
anti-spoofing gateway-disguiser	ARP Gateway anti-spoofing function enable state
arp anti-spoofing source-mac-check	ARP Enable state of packet source address consistency check function

44.2.2 show arp anti-spoofing bind

【command】

show arp anti-spoofing bind

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show arp anti-spoofing bind Command is used to view the protected hosts.

【example】

#View protected hosts.

Switch(config)#show arp anti-spoofing bind

Information Arp Anti-Spoofing Bind:

Enable arp anti-spoofing to make bind ip take effect.

Depend on arp anti-spoofing known-packet policy and unknown-packet policy.

Max entry allowed to bind: 1024

IpAddress Port

1.1.1.1 e0/0/1

Total entries: 1. Printed entries: 1.

arp anti-spoofing bind display field description

Field	Description
Max entry allowed to bind	Maximum number of hosts allowed to be bound by ARP anti-flooding protection
IpAddress	Host IP address
Port	Port number

44.2.3 show arp anti-attack

【command】

show arp anti-attack [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show arp anti-attack Command to view the trusted ports.

【example】

#View Trusted Ports.

Switch(config)#show arp anti-attack

Port informations of arp anti-attack

Port	Mode	Rate-limit(anti-flood)
e0/0/1	untrust	-
e0/0/2	untrust	-
e0/0/3	untrust	-
e0/0/4	untrust	-
e0/0/5	untrust	-
e0/0/6	untrust	-

arp anti-attack display field description

Field	Description
Port	Port number
Mode	Port Mode: trust、untrust
Rate-limit(anti-flood)	Flood control rate

Chapter 45 ARP anti-flood

45.1 ARP anti-flood configuration commands

45.1.1 arp anti-flood

【command】

arp anti-flood

no arp anti-flood

【config-mode】

Global configuration mode

【parameter】

None

【description】

arp anti-flood Command to enable the flood prevention function.

no arp anti-flood Command to disable the flood prevention function.

By default, arp anti-flood is disabled. After enabling the function, ARP packets exceeding the specified rate will be treated as attackers.

Anti-ARP flooding is used to prevent attackers from using a large number of ARP request packets to attack the gateway or server, preventing the CPU resources of the network equipment from being consumed due to the above attacks, thus affecting the forwarding of normal service packets.

【example】

#Enabling arp flooding prevention mechanism.

Switch#configure terminal

Switch(config)#arp anti-flood

45.1.2 arp anti-flood action

【command】

arp anti-flood action { deny-all | deny-arp }

no arp anti-flood action

【config-mode】

Global configuration mode

【parameter】

deny-all: Indicates that all packets from the attacker are dropped.

deny-arp: Indicates that only the attacker's arp packets are dropped, the default method.

【description】

arp anti-flood action Command is used to configure the processing behavior of ARP attack packets.

no arp anti-flood action Command is used to restore the default processing behavior deny-arp.

【example】

#Configure the processing behavior for ARP attack packets to deny-all.

Switch#configure terminal

Switch(config)#arp anti-flood action deny-all

45.1.3 arp anti-flood rate-limit

【command】

arp anti-flood rate-limit *rate-limit-value*

no arp anti-flood rate-limit

【config-mode】

Global configuration mode/Port Configuration Mode

【parameter】

rate-limit-value: Speed limit value, in integer form, in the range of 1 to 100, unit is pps.

【description】

arp anti-flood rate-limit Command is used to configure the arp rate threshold.

no arp anti-flood rate-limit Command is used to restore the default value.

By default, the global threshold is 16pps and the port threshold is 0pps, indicating that the global threshold is used. When the port threshold is non-zero, the port threshold is used first.

After enabling arp anti-flood, if the ARP rate is less than the arp anti-flood rate-limit threshold, the system will not consider it an attack and forward this ARP packet normally; if the rate is greater than the arp anti-flood rate-limit threshold, it will consider it an attack and handle it according to the behavior configured by arp anti-flood action.

【example】

Configure the global arp rate threshold to 100pps.

Switch#configure terminal

Switch(config)#arp anti-flood rate-limit 100

45.1.4 arp anti-flood recover-time

【command】

arp anti-flood recover-time *recover-time-value*

no arp anti-flood recover-time

【config-mode】

Global configuration mode

【parameter】

recover-time-value: Recovery time, in the form of an integer, takes the value range 0-1440, default 10, unit is minutes.

0 means no automatic recovery, manual recovery is required.

【description】

arp anti-flood recover-time Command is used to configure the disabled user auto recovery time.

no arp anti-flood recover-time Command is used to restore the default value.

By default, the automatic recovery time for forbidden users is 10 min. When an attack is detected, the system sends the attacker down to the attack table entry to forbid communication. Use this command to modify the time for forbidden users to automatically resume communication.

【example】

#Configure the automatic recovery time for prohibited users to 100min.

Switch#configure terminal

Switch(config)#arp anti-flood recover-time 100

45.1.5 arp anti-flood recover

【command】

arp anti-flood recover { all | *mac-address-value* **}**

【config-mode】

Global configuration mode

【parameter】

all: All forbidden users.

mac-address-value: MAC address, colon in hexadecimal form.

【description】

arp anti-flood recover Command is used to manually restore the forbidden user.

This command allows the attacker to resume communication immediately after being sent to the forbidden user list.

【example】

#Manually restore all forbidden users.

Switch#configure terminal

Switch(config)#arp anti-flood recover all

45.1.6 arp anti-flood bind blackhole

【command】

arp anti-flood bind blackhole { all | *mac-address-value* **}**

【config-mode】

Global configuration mode

【parameter】

all: All forbidden users.

mac-address-value: MAC address, colon in hexadecimal form.

【description】

arp anti-flood bind blackhole Command is used to bind the forbidden user to a static blackhole MAC,This command can only be used when Action is deny-all.

【example】

#Bind all forbidden users to a static black hole MAC.

Switch#configure terminal

Switch(config)#arp anti-flood bind blackhole all

45.2 ARP anti-flood monitoring commands

45.2.1 show arp anti-flood

【command】

show arp anti-flood

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show arp anti-flood command to view the arp anti-flooding configuration information and the issued attack table entries.

【example】

#View arp flood control configuration.

Switch(config)#show arp anti-flood

Informations of arp anti-flood

Arp anti-flood: enabled

Arp anti-flood rate-limit: 16pps

Arp anti-flood user recovery time: 10 minutes

Arp anti-flood deny type: DenyARP

DeniedSrcMAC SourceIP Port Vlan DenyType RemainAgingTime(m: s)

Total entries: 0.

arp anti-flood display field description.

Field	Description
Arp anti-flood	ARP anti-flooding function enable state
Arp anti-flood rate-limit	ARP anti-flooding rate limiting
Arp anti-flood user recovery time	Automatic recovery time for banned users
Arp anti-flood deny type	Processing behavior: DenyARP, DenyALL
DeniedSrcMAC	Blocked Source MAC
SourceIP	Blocked source IP
Port	Port number
Vlan	VLAN id
DenyType	Processing behavio: DenyARP、DenyALL

RemainAgingTime(m: s)	Remaining recovery time (minutes and seconds)

45.2.2 show arp anti-flood rate-limit

【command】

show arp anti-flood rate-limit

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show arp anti-flood rate-limit Command is used to view the arp rate threshold.

【example】

#View arp rate threshold.

Switch(config-if-ethernet-0/0/1)#show arp anti-flood rate-limit

Informations of arp anti-flood

Arp anti-flood: enabled

Arp anti-flood rate-limit: 16pps

Arp anti-flood user recovery time: 10 minutes

Arp anti-flood deny type: DenyARP,Ports use the global rate-limit if not specify value

Port	Rate-limit
e0/0/1	0
e0/0/2	0
e0/0/3	0

e0/0/4 0

arp anti-flood rate-limit display field description.

Field	Description
Arp anti-flood	ARP anti-flooding function enable state
Arp anti-flood rate-limit	ARP anti-flooding rate limiting
Arp anti-flood user recovery time	Automatic recovery time for forbidden users
Arp anti-flood deny type	Processing behavio: DenyARP、DenyALL
Port	Port number
Rate-limit	ARP anti-flooding rate threshold

Chapter 46 Attack detection

46.1 Attack detection configuration commands

46.1.1 cpu-car

【command】

cpu-car *rate-value*

no cpu-car

【config-mode】

Global configuration mode

【parameter】

rate-value: CPU processing rate threshold, the value range is 1-10000pps, the default value is 2000pps.

【description】

cpu-car Command is used to configure the CPU processing rate threshold.

no cpu-car Command to restore the CPU processing rate to the default value.

【example】

#Configure the processing rate of the cpu to 1000pps.

Switch#configure terminal

Switch(config)#cpu-car 1000

46.1.2 alarm cpu

【command】

alarm cpu

no alarm cpu

【config-mode】

Global configuration mode

【parameter】

None

【description】

alarm cpu Command to enable cpu alarm.

no alarm cpu Command to disable cpu alarm.

Default enable cpu alarm function.

【example】

#Enable cpu alarm.

Switch#configure terminal

Switch(config)#alarm cpu

46.1.3 alarm cpu threshold busy

【command】

alarm cpu threshold { busy | unbusy } *threshold-value*

no alarm cpu threshold

【config-mode】

Global configuration mode

【parameter】

busy: Indicates the threshold for configuring cpu busy.

unbusy: Indicates the threshold value for configuring cpu idle.

threshold-value: Threshold, in integer form, from 0 to 100, in %. busy default threshold 90%, unbusy default threshold 60%.

【description】

alarm cpu threshold Command is used to configure the cpu alarm threshold.

no alarm cpu threshold Command restores the default value of cpu alarm threshold.

When CPU utilization reaches the busy threshold, a cpu busy log message is generated; when CPU utilization returns to the

unbusy threshold, a cpu unbusy log message is generated.

【example】

#Configure the cpu busy alarm threshold to 80%.

Switch#configure terminal

Switch(config)#alarm cpu threshold busy 80

46.1.4 alarm all-packets

【command】

alarm all-packets

no alarm all-packets

【config-mode】

Global configuration mode/Port Configuration Mode

【parameter】

None

【description】

alarm all-packets Command to enable port alerting.

no alarm all-packets Command is used to disable port alarms.

Port alarm function is enabled by default.

【example】

#Enable all port alarms.

Switch#configure terminal

Switch(config)#alarm all-packets

46.1.5 alarm all-packets threshold

【command】

alarm all-packets threshold { exceed | normal } *threshold-value*

no alarm all-packets threshold

【config-mode】

Port Configuration Mode

【parameter】

exceed: Indicates the threshold for configuring a port to be busy.

normal: Indicates the threshold value for configuring the port to return to normal.

threshold-value: Threshold, integer form, in the range of 1-1000, in Mbps.

【description】

alarm all-packets threshold Command is used to configure the port alarm threshold.

no alarm all-packets threshold Command restores the port alarm threshold default value.

exceed the default threshold of 850M, normal the default threshold of 600M.

When the port rate reaches the excepted threshold, the log message of excepted will be generated; when the port rate returns to the normal threshold, the log message of normal will be generated.

【example】

#Configure the exceed alarm threshold for port 1 to 900M.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch#(config-if-ethernet-0/0/1)#alarm all-packets threshold exceed 900

46.1.6 system trap { enable | disable }

【command】

system trap { enable | disable }

【config-mode】

Global configuration mode

【parameter】

enable: Indicates the enable function.

disable: Indicates disable function.

【description】

system trap enable Command enables the trap message reporting function of cpu utilization and memory status.

system trap disable Command is used to restore the default configuration.

By default, the trap message reporting function of cpu utilization and memory status is disabled.

【example】

#Enable the trap message reporting function for cpu utilization and memory situation.

Switch#configure terminal

Switch(config)#system trap enable

46.1.7 system trap period

【command】

system trap period *period-value*

no system trap period

【config-mode】

Global configuration mode

【parameter】

period-value: Notification period, integer form, the value range is 1-600, default 300, unit of seconds.

【description】

system trap period Command is used to configure the trap information reporting period.

no system trap period Command is used to restore the default configuration.

By default, the reporting period is 300 seconds.

【example】

#Configure the reporting period to 600s.

Switch(config)#system trap period 600

46.1.8 port-car

【command】

port-car

no port-car

【config-mode】

Global configuration mode/port configuration mode

【parameter】

None

【description】

port-car Command is used to enable the port-car function.

no port-car Command is used to disable the port-car function.

By default, the port-car function is enabled.

【example】

#Global enable port-car function.

Switch#configure terminal

Switch(config)#port-car

46.1.9 port-car rate

【command】

port-car rate *rate-value*

no port-car rate *rate-value*

【config-mode】

Global configuration mode/port configuration mode

【parameter】

rate-value: Threshold, global value range 1-3000, port value range 1-128, unit pps.

【description】

port-car rate Command is used to configure the rate of processing BPDU packets.

no port-car rate Command is used to restore the default values.

By default, the global processing rate is 1200pps and the port processing rate is 30pps.

【example】

#Configure the global port-car rate to 60pps.

Switch#configure terminal

Switch(config)#port-car rate 60

46.1.10 bpdu-discard

【command】

bpdu-discard

no bpdu-discard

【config-mode】

Global configuration mode

【parameter】

None

【description】

bpdu-discard Command enables to discard bpdu packets.

no bpdu-discard Command is used to turn off dropping bpdu packets and restore the default configuration.

When the function is enabled, the system will discard the received bpdu packets.

【example】

#Enable bpdu-discard.

Switch(config)#bpdu-discard

46.1.11 anti-dos packets class

【command】

anti-dos packets class { type0 | type1 | type2 | type3 | type4 | type5 | type6 | type7 | type8 type9 | type10 | type11 | type12 | type13 | type14 }

no anti-dos packets class anti-dos packets class { type0 | type1 | type2 | type3 | type4 | type5 | type6 | type7 | type8 type9 | type10 | type11 | type12 | type13 | type14 }

【config-mode】

Global configuration mode

【parameter】

type0: Source MAC and dst MAC equal

type1: Source IP and dst IP equal

type10: Fragmented ICMP packets

type11: TCP fragments with offset value of 1(*8)

type12: TCP with SYN & FIN bits

type13: TCP with FIN,URG and PSH bits,and sequence equal 0

type14: TCP frist fragments with minimum TCP header length

type2: UDP with sport and dport equal

type3: TCP with sport and dport equal

type4: ICMPv4 maxinum length

type5: ICMPv6 maxinum length

type6: TCP control flags and sequence equal 0

type7: TCP SYN flags unviable

type8: Check IP first fragments

type9: Minimum size of IPv6 fragments

【description】

anti-dos packets class Command is used to enable the specified type of anti-attack.

no anti-dos packets class type Command is used to disable the specified type of anti-attack.

By default, all types of anti-attack are disabled.

【example】

#Enable anti-dos attack type0.

Switch(config)#anti-dos packets class type0

46.1.12 dhcp anti-attack

【command】

dhcp anti-attack

no dhcp anti-attack

【config-mode】

Global configuration mode

【parameter】

None

【description】

dhcp anti-attack Command to enable anti-dhcp attack function.

no dhcp anti-attack Command to disable the anti-dhcp attack function.

By default, the anti-dhcp attack function is disabled.

【example】

#Enable anti-dhcp attack function.

Switch#configure terminal

Switch(config)#dhcp anti-attack

46.1.13 dhcp anti-attack action

【command】

dhcp anti-attack action { deny-all | deny-dhcp } [threshold *threshold-value* **]**

【config-mode】

Global configuration mode

【parameter】

deny-all: Indicates that all packets are discarded.

deny-dhcp: Indicates that dhcp packets are discarded and the default configuration is restored.

threshold-value: Threshold value, the range is 1-100, the default value is 16, unit pps.

【description】

dhcp anti-attack action Command is used to configure the processing action for anti-dhcp attack.

By default, the processing action for anti-dhcp attack is to reject dhcp packets.

After enabling dhcp anti-attack, if the DHCP rate is less than the dhcp anti-attack threshold, the system will not consider it an attack and forward this DHCP packet normally; if the rate is greater than the dhcp anti-attack threshold, it will consider it an attack and handle it according to the behavior configured by dhcp anti-attack action..

【example】

#Configure action to discard all packets.

Switch#configure terminal

Switch(config)#dhcp anti-attack action deny-all

46.1.14 dhcp anti-attack bind blackhole

【command】

dhcp anti-attack bind blackhole { all | *mac-value* **}**

【config-mode】

Global configuration mode

【parameter】

all: Bind all denied mac addresses as black hole mac addresses.

mac-value: Bind the designated denied address as the black hole mac address.

【description】

dhcp anti-attack bind blackhole Command is used to configure the binding black hole mac function.

After enabling dhcp anti-attack, the attack packets will be generated to reject table entries, and after configuring binding black hole mac address, the packets matching the black hole mac address will be dropped.

【example】

#Bind the rejected 00: 00: 00: 11: 22: 33 address to the black hole mac address.

Switch#configure terminal

Switch(config)#dhcp anti-attack bind blackhole 00: 00: 00: 11: 22: 33

46.1.15 dhcp anti-attack threshold

【command】

dhcp anti-attack threshold *threshold-value*

no dhcp anti-attack threshold

【config-mode】

Global configuration mode/Port Configuration Mode

【parameter】

threshold-value: Threshold value, the range is 1-100, the default value is 16, unit pps.

【description】

dhcp anti-attack threshold Command is used to configure the attack threshold.

no dhcp anti-attack threshold Command is used to restore the default values.

After enabling dhcp anti-attack, if the DHCP rate is not greater than the dhcp anti-attack threshold, the system will not consider it as an attack and forward this DHCP packet normally; if the rate is greater than the dhcp anti-attack threshold, it will consider it as an attack and handle it according to the behavior configured by dhcp anti-attack action.

【example】

#Configure the global dhcp anti-attack threshold to 20pps.

Switch#configure terminal

Switch(config)#dhcp anti-attack threshold 20

46.1.16 dhcp anti-attack recover-time

【command】

dhcp anti-attack recover-time *time-value*

no dhcp anti-attack recover-time

【config-mode】

Global configuration mode

【parameter】

time-value: Auto recovery time, the value range is 0-1440, the default value is 10, unit min.

【description】

dhcp anti-attack recover-time Command is used to configure the automatic recovery time.

no dhcp anti-attack recover-time Command to restore the automatic recovery time to the default value.

After enabling the function, the system deletes the dhcp attack table entry after the automatic recovery time, and when the automatic recovery time is configured to 0min, the table entry disables the automatic recovery function, that is, the dhcp attack table entry is never deleted.

【example】

#Configure automatic recovery time to 1min.

Switch#configure terminal

Switch(config)#dhcp anti-attack recover-time 1

46.1.17 dhcp anti-attack recover

【command】

dhcp anti-attack recover { **all** | *mac-value* }

【config-mode】

Global configuration mode

【parameter】

all: Manually restore all table entries.

mac-value: Manually restore the specified mac table entry.

【description】

dhcp anti-attack recover Command to configure manual recovery of dhcp attack table entries.

【example】

#Manually restore the dhcp attack table entry with mac address 00: 00: 00: 11: 22: 33.

Switch#configure terminal

Switch(config)#dhcp anti-attack recover 00: 00: 00: 11: 22: 33

46.1.18 dhcp anti-attack trust

【command】

dhcp anti-attack trust

no dhcp anti-attack trust

【config-mode】

Port Configuration Mode

【parameter】

None

【description】

dhcp anti-attack trust Command is used to enable the port as a trusted port.

no dhcp anti-attack trust Command is used to configure the port as an untrusted port.

After configured as a trusted port, dhcp packets received above the threshold will not be treated as attack packets.

【example】

#Configure port ethernet 0/0/1 as a trust port.

Switch#configure terminal

Switch(config-if-ethernet-0/0/1)#dhcp anti-attack trust

46.1.19 cpu-attack threshold

【command】

cpu-attack protect

no cpu-attack protect

【config-mode】

Port Configuration Mode

【parameter】

None

【description】

cpu-attack protect Command to enable CPU attack protection.

no cpu-attack protect Command the user to disable CPU attack protection.

By default, it is enabled to discard telegrams when receiving attacks on the CPU to prevent malicious protocol packets from attacking in the network, causing the CPU of the device to be over-utilized and causing the device to fail to operate normally.

【example】

#Under port ethernet 0/0/1, enable CPU attack protection.

Switch#configure terminal

Switch(config-if-ethernet-0/0/1)#cpu-attack protect

46.1.20 cpu-attack protect

【command】

cpu-attack protect

no cpu-attack protect

【config-mode】

Port Configuration Mode

【parameter】

None

【description】

cpu-attack protect Command to enable CPU attack protection.

no cpu-attack protect Command the user to disable CPU attack protection.

By default, it is enabled to discard telegrams when receiving attacks on the CPU to prevent malicious protocol packets from attacking in the network, causing the CPU of the device to be over-utilized and causing the device to fail to operate normally.

【example】

#Under port ethernet 0/0/1, enable CPU attack protection.

Switch#configure terminal

Switch(config-if-ethernet-0/0/1)#cpu-attack protect

46.1.21 cpu-ratelimit

【command】

cpu-ratelimit queue *queue-value* **limit** *limit-value*

no cpu-ratelimit queue *queue-value* **limit**

【config-mode】

Global configuration mode

【parameter】

queue-value: Configure the queue number of the CPU queue, the value range is 0-7, corresponding to the queue of each protocol.

limit-value: Rate threshold, the value range is 1-20000, the unit is pps. the default value is as follows:

queue 0: limit 640pps

queue 1: limit 640pps

queue 2: limit 1024pps

queue 3: limit 1024pps

queue 4: limit 512pps

queue 5: limit 1024pps

queue 6: limit 1024pps

queue 7: limit 1024pps

【description】

cpu-ratelimit queue Command configures the rate at which the CPU queue processes protocol packets.

no cpu-ratelimit queue Command to restore the CPU queue processing rate of protocol packets to the default value.

The device is able to limit the CPU packet processing rate per queue to prevent malicious protocol packet attacks in the network from over-utilizing the CPU of the device and causing the device to fail to operate normally.

【example】

#Limit the rate of CPU queue 0 to 100pps.

Switch#configure terminal

Switch(config)#cpu-ratelimit queue 0 limit 100

46.1.22 ip dlf cpu

【command】

ip dlf cpu

no ip dlf cpu

【config-mode】

Global configuration mode

【parameter】

None

【description】

ip dlf cpu Command to enable CPU processing on ip unknown packets.

no ip dlf cpu Command to disable CPU processing on ip unknown packets.

Enable ip dlf cpu by default, use flow forwarding mode (packets with failed route find or unreachable destination will be sent to CPU for further processing).

【example】

#Enable ip dlf cpu .

Switch#configure terminal

Switch(config)#ip dlf cpu

46.1.23 ip host-dlf cpu

【command】

ip host-dlf cpu

no ip host-dlf cpu

【config-mode】

VLAN interface configuration mode

【parameter】

None

【description】

ip host-dlf cpu Command enables CPU processing on ip host unknown packets.

no ip host-dlf cpu Command to disable CPU processing on ip host unknown packets.

Enable ip host-dlf cpu by default, use flow forwarding mode (packets with failed route finds or unreachable destinations will be sent to CPU for further processing).

【example】

#Enable ip host-dlf cpu .

Switch#configure terminal

Switch#(config)#interface vlan-interface 1

Switch(config-if-vlanInterface-1)#ip host-dlf cpu

46.2 Attack detection monitoring commands

46.2.1 show cpu-car

【command】

show cpu-car

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show cpu-car Command to view cpu-car configuration information.

【example】

#View cpu-car configuration information.

Switch#configure terminal

Switch(config)#show cpu-car

Send packet to cpu rate = 2000 pps.

46.2.2 show cpu-statistics

【command】

show cpu-statistics [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, configuration range determined by hardware type.

【description】

show cpu-statistics Command is used to view the CPU packet receiving information astatistics.

【example】

#View port 0/0/1 CPU packet receipt information statistics.

Switch#configure terminal

Switch(config)#show cpu-statistics ethernet 0/0/1

Port number : e0/0/1

Input : 0 packets, 0 drops, 0 bpdu

0 broadcasts, 0 multicasts, 0 unicasts

0 64Bytes, 0 128Bytes, 0 256Bytes

0 512Bytes, 0 1024Bytes, 0 2048Bytes, 0 2048Bytes Over

cpu-statistics display field description

Field	Description
Port number	Port number
Input	Input Data Packets: Total data packets, drops: Dropped data packets bpdu: Bpdu data packet， broadcasts: Broadcast packets multicasts: Multicasts packets， unicasts: Unicasts packets 64Bytes: Number of packets received by the CPU for 64

	bytes 128Bytes: Number of packets received by the CPU for 128 bytes 256Bytes: Number of packets received by the CPU for 256 bytes 512Bytes: Number of packets received by the CPU for 512 bytes 1024Bytes: Number of packets received by the CPU for 1024 bytes 2048Bytes: Number of packets received by the CPU for 2048 bytes 2048Bytes Over: Number of CPU packets received greater than 2048 bytes

46.2.3 clear cpu-statistics

【command】

clear cpu-statistics

【config-mode】

Global configuration mode

【parameter】

None

【description】

clear cpu-statistics Command to clear cpu packet receipt statistics.

【example】

#Clear cpu packet receipt statistics.

Switch#configure terminal

Switch(config)#clear cpu-statistics

46.2.4 show cpu-classification

【command】

show cpu-classification [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, configuration range determined by hardware type.

【description】

show cpu-classification Command to view cpu packet receipt statistics

【example】

#View cpu packet receipt statistics by category.

Switch#configure terminal

Switch(config)#show cpu-classification

Type	Count	Percent(%)
Total	316	100
BPDU	0	0
EIPS	0	0
ARP	299	94
MLD	0	0
IGMP	0	0
ICMP	0	0
DHCP	0	0
SNMP	0	0

Telnet 0 0

SSH 0 0

Other 17 5

cpu-classification display field description

Field	Description
Type	Statistical classification
Count	Number of packages received
Percent(%)	Percentage of packages received

46.2.5 clear cpu-classification

【command】

clear cpu-classification [ethernet *port-id* **]**

【config-mode】

Privileged user/global configuration mode

【parameter】

port-id: Port number, configuration range determined by hardware type.

【description】

clear cpu-classification Command to clear cpu packet receipt classification statistics.

【example】

#Clear cpu category statistics.

Switch#configure terminal

Switch(config)#clear cpu-classification

46.2.6 show cpu-utilization

【command】

show cpu-utilization

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show cpu-utilization Command to view cpu utilization.

【example】

#Display CPU utilization information.

Switch#configure terminal

Switch(config)#show cpu-utilization

CPU Information:

CPU Idle : 95 %

46.2.7 show port-car

【command】

show port-car

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show port-car Command displays the global and port-car enable status and the suppression rate of the port.

【example】

#View port-car configuration information.

Switch#show port-car

Port CAR global status: enable

Port CAR rate(PPS): 1200pps

Port CAR port informations:

port status port-car rate

e0/0/1 enable 20

e0/0/2 enable 30

e0/0/3 enable 30

e0/0/4 enable 30

e0/0/5 enable 30

port-car display field description

Field	Description
Port CAR global status	Global enable state
Port CAR rate(PPS)	Global suppression rate
port	Port number
status	Port enable state
port-car rate	Port rejection rate

46.2.8 show anti-dos

【command】

show anti-dos

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show anti-dos Command to view the anti-dos configuration.

【example】

#View anti-dos configuration.

Switch(config)#show anti-dos

Informations of AntiDos:

anti-dos packets class type0

46.2.9 show bpdu-discard

【command】

show bpdu-discard

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show bpdu-discard Command is used to view the bpdu-discard configuration.

【example】

#View bpdu-discard configuration.

Switch(config)#show bpdu-discard

Global bpdu-discard : enable

46.2.10 show dhcp anti-attack

【command】

show dhcp anti-attack

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show dhcp anti-attack Command to view dhcp anti-attack configuration status.

【example】

#View dhcp anti-attack status.

Switch(config)#show dhcp anti-attack

Informations of dhcp anti attack

Dhcp anti-attack: disabled

Dhcp rate limit: 16pps

User recovery time: 10 minutes

Reject type: DenyDHCP

DeniedSrcMAC Port Vlan DenyType RemainAgingTime(m)

Total entries: 0.

dhcp anti-attack display field description

Field	Description
DeniedSrcMAC	Rejected source MAC
Port	Port number
Vlan	VLAN id
DenyType	Discard Type: DenyAll、DenyDHCP
RemainAgingTime(m)	Remaining recovery time (minutes)
Total entries	Attack table entry statistics

46.2.11 show dhcp anti-attack interface

【command】

show dhcp anti-attack interface [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, configuration range determined by hardware type.

【description】

show dhcp anti-attack interface Command to view the configuration status of port dhcp attack.

【example】

#View port dhcp anti-attack configuration.

Switch#show dhcp anti-attack interface

Port informations of dhcp anti attack trust

Port	mode	threshold
e0/0/1	untrust	-
e0/0/2	untrust	-
e0/0/3	untrust	-
e0/0/4	untrust	-

show dhcp anti-attack interface display field description

Field	Description
Port	Port number
mode	Trust model: trust、untrust
threshold	Rate Threshold

46.2.12 show alarm cpu

【command】

show alarm cpu

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show alarm cpu Command to view cpu alarm information.

【example】

#View cpu alarm information.

Switch#show alarm cpu

CPU status alarm : disable

CPU busy threshold(%) : 90

CPU unbusy threshold(%) : 60

CPU status : unbusy

show alarm cpu display field description

Field	Description
CPU status alarm	Enabled state
CPU busy threshold(%)	Busy threshold
CPU unbusy threshold(%)	Unbusy threshold
CPU status	Status

46.2.13 show alarm all-packets

【command】

show alarm all-packets

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show alarm all-packets Command to view port alarm status information.

【example】

#View port alarm status information.

Switch#show alarm all-packets

Port alarm global status : enable

Port alarm exceed port :

show alarm all-packets display field description

Field	Description
Port alarm global status	Enabled state
Port alarm exceed port	List of ports that exceed the threshold

46.2.14 show alarm all-packets interface

【command】

show alarm all-packets interface [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, configuration range determined by hardware type.

【description】

show alarm all-packets interface Command to view port alarm configuration information.

【example】

#View port alert configuration information.

Switch#show alarm all-packets interface ethernet 0/0/1

e0/0/1 port alarm information

Port alarm status : enable

Port alarm exceed threshold(Mbps) : 850

Port alarm normal threshold(Mbps) : 600

show alarm all-packets interface display field description

Field	Description
Port alarm status	Enabled state
Port alarm exceed threshold(Mbps)	Alarm threshold exceeded
Port alarm normal threshold(Mbps)	Restore alarm thresholds

46.2.15 show ip dlf cpu

【command】

show ip dlf cpu

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show ip dlf cpu Command to view ip dlf cpu enable status.

【example】

#View ip dlf cpu status information.

Switch#configure terminal

Switch(config)#show ip dlf cpu

Ip dlf cpu : enable.

46.2.16 show ip host-dlf cpu

【command】

show ip host-dlf cpu

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show ip host-dlf cpu Command to view ip host-dlf cpu status information.

【example】

#View ip host-dlf cpu status information.

Switch#configure terminal

Switch(config)#show ip host-dlf cpu

Interface : Host dlf cpu

VLAN-IF1 : Enabled

46.2.17 show cpu-attack interface

【command】

show cpu-attack interface [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, configuration range determined by hardware type.

【description】

show cpu-attack interface Command to view cpu-attack configuration information.

【example】

#View the cpu-attack configuration information of port 0/0/1.

Switch(config)#show cpu-attack interface

cpu auto protect informations:

token bucket threshold : 8000

recover normal tokens : 2500

stage take tokens : 90

init bucket tokens : 500

port : enable

e0/0/1 : Enable

e0/0/2 : Enable

show cpu-attack display field description

Field	Description
token bucket threshold	Threshold
recover normal tokens	Return to normal

stage take tokens	Storage size
init bucket tokens	Initial size
port	Port number
enable	Enabled state

Chapter 47 IP-source-guard

47.1 ip-source-guard configuration command

47.1.1 ip source

【command】

ip source [ip | ip-mac | ip-mac-vlan]

no ip source

【config-mode】

port configuration mode

【parameter】

ip: Represents filtering of messages based on ip address.

ip-mac: represents filtering of messages based on ip+mac.

ip-mac-vlan: Represents filtering of messages based on ip+mac+vlan.

【description】

ip source [ip-mac-vlan] Command to enable ip-mac-vlan filtering.

ip source ip Command to enable the ip filtering method.

ip source ip-mac Command to enable ip-mac filtering method.

no ip source Command to restore the default configuration.

By default, the port disables the ip source guard function.

When ip source is enabled, only messages matching the bind table entry or dhcp snooping table entry can be forwarded, other messages will be discarded.

【example】

#Port 2 enables ip-mac filtering.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/2

Switch(config-if-ethernet-0/0/2)#ip source ip-mac

47.1.2 ip source bind

【command】

ip source bind *ip-address [mac-address* **[interface ethernet** *port-id* **vlan** *vlan-id* **]]**

no ip source bind { all | *ip-address* **}**

【config-mode】

Global configuration mode

【parameter】

ip-address: IP address, dotted decimal, format: X.X.X.

mac-address: MAC address, in bold hexadecimal, format: X: X: X: X: X: X.

port-id: Port number, based on the physical port of the switch.

vlan-id: VLAN number, value range 1-4094.

【description】

ip source bind Command to configure IP Source Guard binding table entries.

no ip source bind Command to delete the IP Source Guard binding table entry.

By default, no port IP Source Guard binding table entry exists.

When the IP source guard function is enabled on a port, messages that match the binding table entry can be forwarded, and messages that do not match the binding table entry are discarded.

【example】

#Configure IP source guard binding table entries: IP=1.1.1.1, MAC=10: 01: 01: 01: 01: 01, port=0/0/1, vlan=2.

Switch#configure terminal

Switch(config)#ip source bind 1.1.1.1 10: 01: 01: 01: 01: 01 interface ethernet 0/0/1 vlan 2

47.1.3 ip source vlan

【command】

ip source vlan *vlan-id*

no ip source vlan *vlan-id*

【config-mode】

Global configuration mode

【parameter】

vlan-id: VLAN number, value range 1-4094.

【description】

ip source vlan The command enables the filtering function of vlan.

no ip source vlan Command to disable filtering for vlan.

By default, the filtering function of vlan is enabled.

【example】

#Disable filtering on vlan2.

Switch#configure terminal

Switch(config)#no ip source vlan 2

47.1.4 ip source permit-igmp

【command】

ip source permit-igmp

no ip source permit-igmp

【config-mode】

Global configuration mode

【parameter】

None

【description】

ip source permit-igmp Command to enable forwarding of igmp protocol packets.

no ip source permit-igmp Command to restore the default configuration.

By default, igmp protocol packets are discarded.

【example】

#Enables forwarding of igmp protocol packets.

Switch#configure terminal

Switch(config)ip source permit-igmp

47.2 ip-source-guard monitor command

47.2.1 show ip source bind

【command】

show ip source bind [*ip-address***]**

【config-mode】

arbitrary configuration mode

【parameter】

ip-address: IP address in dotted decimal, format: X.X.X.

【description】

show ip source bind Command to view the binding table entries.

【example】

#View binding table entries.

Switch(config)#show ip source binding

IP	MAC	PORT	VLAN
1.1.1.1	10: 01: 01: 01: 01: 01	GE0/0/1	2

Total entries: 1.

ip source bind display field description

Field	Description
IP	Binding table entry source IP address
MAC	Binding table entry source MAC address
PORT	The port number corresponding to the binding table entry
VLAN	The VLAN number corresponding to the binding table entry

47.2.2 show ip source vlan

【command】

show ip source vlan

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show ip source vlan Command to view vlan filtering configuration information.

【example】

#View vlan filtering configuration information.

Switch(config)#show ip source vlan

IP Source Guard is disabled in following vlans: 2

47.2.3 show ip source permit-igmp

【command】

show ip source permit-igmp

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show ip source permit-igmp Command to display permit-igmp configuration information.

【example】

#View permit-igmp configuration information.

Switch(config)#show ip source permit-igmp

IP source guard permit igmp status: enable

47.2.4 show ip source

【command】

show ip source

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show ip source The command displays the port filtering method configuration information.

【example】

#View port filtering configuration information.

Switch(config)#show ip source

Port Status FilterType

e0/0/1 disable N/A

e0/0/2 disable N/A

e0/0/3 disable N/A

e0/0/4 disable N/A

……

ip source display field description

Field	Description
Port	Port number
Status	Enabling status: disable, enable
FilterType	Filter: ip, ip-mac, ip-mac-vlan N/A: indicates Status=disable;

Chapter 48 DHCP-snooping

48.1 dhcp-snooping configuration command

48.1.1 dhcp-snooping

【command】

dhcp-snooping

no dhcp-snooping

【config-mode】

Global/VLAN configuration mode

【parameter】

None

【description】

dhcp-snooping Command is used to enable the function.

no dhcp-snooping Command to restore the default situation.

By default, the global DHCP Snooping function is disabled and the DHCP snoping function under VLAN is enabled.

【example】

#Enabling DHCP Snooping.

Switch#configure terminal

Switch(config)#dhcp-snooping

48.1.2 dhcp-snooping trust

【command】

dhcp-snooping trust

no dhcp-snooping trust

【config-mode】

Port/VLAN configuration mode

【parameter】

None

【description】

dhcp-snooping trust Command to configure trust mode.

no dhcp-snooping trust Command to restore the default situation.

By default, all ports/VLANs are in untrusted mode.

The port connected to the DHCP server needs to be configured in trusted mode, otherwise the DHCP client will not be able to obtain the address.

【example】

#Configure port ethernet 0/0/1 as trusted mode.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#dhcp-snooping trust

48.1.3 dhcp-snooping fast-remove

【command】

dhcp-snooping fast-remove

no dhcp-snooping fast-remove

【config-mode】

Global configuration mode

【parameter】

fast-remove: Represents the immediate deletion of DHCP listener table entries when the port is disconnected.

【description】

dhcp-snooping fast-remove The command is used to enable the fast-remove function.

no dhcp-snooping fast-remove Command to disable the fast-remove function.

By default, the fast-remove function is enabled.

【example】

#Disable the fast-remove function.

Switch#configure terminal

Switch(config)#dhcp-snooping fast-remove

48.1.4 dhcp-snooping max-learn-num

【command】

dhcp-snooping max-learn-num *max-value*

no dhcp-snooping max-learn-num

【config-mode】

Port/VLAN configuration mode

【parameter】

max-value: Number of clients, in the range 0-2048, default 2048.

【description】

dhcp-snooping max-learn-num The command is used to configure the maximum number of users allowed to connect to the port.

no dhcp-snooping max-learn-num Command to restore the default value.

By default, the default value is 2048.

【example】

#Configure port 0/0/1 with a maximum learning quantity of 20.

Switch#configure terminal

Switch#(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#dhcp-snooping max-learn-num 20

48.1.5 dhcp-snooping dhcp-server

【command】

dhcp-snooping dhcp-server *ip-address*

no dhcp-snooping dhcp-server { all | *ip-address* **}**

【config-mode】

Global configuration mode

【parameter】

ip-address: ip address, dotted decimal, format: X.X.X.X.

【description】

dhcp-snooping dhcp-server Command to configure the server address.

no dhcp-snooping dhcp-server Command is used to delete the configuration.

After configuring this command, only the client information corresponding to the server will be recorded.

By default there is no server, i.e. all client information is recorded.

【example】

#Configure the server address as 1.1.1.1.

Switch#configure terminal

Switch(config)#dhcp-snooping dhcp-server 1.1.1.1

48.2 dhcp-snooping monitor command

48.2.1 show dhcp-snooping interface

【command】

show dhcp-snooping interface [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, based on the physical port of the switch.

【description】

show dhcp-snooping interface Command to view port configuration information.

【example】

#View the dhcp-snooping configuration information under port e0/0/1

Switch(config)#show dhcp-snooping interface ethernet 0/0/1

Config information of DHCP Snooping:

DHCP Snooping status: Enable

DHCP Snooping port-down-action fast-remove: Disable

Port information:

Port	mode	maxclients	clients(ack)	clients(unack)
e0/0/1	trust	20	0	0

dhcp-snooping interface display field description

Field	Description
DHCP Snooping status	Global enable status: Disable, Enable
DHCP Snooping port-down-action fast-remove	fast-remove enable status: Enable, Disable
Port	Port number
mode	Trust status: untrust, trust
maxclients	Maximum number of users allowed to connect

clients(ack)	Responded to ACK client
clients(unack)	Unresponsive ACK client

48.2.2 show dhcp-snooping vlan

【command】

show dhcp-snooping vlan [*vlan-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

vlan-id: vlan number, value range 1-4094.

【description】

show dhcp-snooping vlan Command to view dhcp-snooping vlan configuration.

【example】

#View dhcp-snooping vlan configuration

Switch(config)#show dhcp-snooping vlan

Config information of DHCP Snooping:

DHCP Snooping status: Enable

VLAN information:

VLAN	enable	mode	maxclients	clients(ack)	clients(unack)
1	TRUE	untrust	2048	0	0

dhcp-snooping vlan display field description

Field	Description
DHCP Snooping status	Global enable status: Disable, Enable
VLAN	VLAN ID
enable	VLAN enable status: TRUE, FALSE
mode	Trust status: untrust, trust
maxclients	Maximum number of users allowed to connect
clients(ack)	Responded to ACK client
clients(unack)	Unresponsive ACK client

48.2.3 show dhcp-snooping clients

【command】

show dhcp-snooping clients

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show dhcp-snooping clients Command to view DHCP Snooping client table entries.

【example】

#View DHCP Snooping client table entries

Switch#configure terminal

Switch(config)#show dhcp-snooping clients

DHCP client information:

d - days, h - hours, m - minutes, s - seconds

IPAddress mac vlan port LeaseTime ExceedTime

Total entries: 0. Printed entries: 0.

dhcp-snooping clients display field description

Field	Description
IPAddress	IP address of the client
mac	Client MAC address
vlan	VLAN number
port	Port number
LeaseTime	Lease Time
ExceedTime	Lease aging time

48.2.4 clear dhcp-snooping

【command】

clear dhcp-snooping { *ip-address* | *mac-address* | **vlan** *vlan-id* | **interface ethernet** *port-id* }

【config-mode】

Global configuration mode

【parameter】

ip-address: IP address, in dotted decimal, format: x.x.x.x.

mac-address: mac address, in bold hexadecimal, format: X: X: X: X: X: X.

vlan-id: VLAN id, value range 1-4094.

port-id: Port number, based on the physical port of the switch.

【description】

clear dhcp-snooping Command to delete table entries of DHCP Snooping records.

【example】

#Delete the table entry for DHCP Snooping vlan 2

Switch#configure terminal

Switch(config)#clear dhcp-snooping vlan 2

48.2.5 debug dhcpsnooping

【command】

debug dhcpsnooping

no debug dhcpsnooping

【config-mode】

Global configuration mode

【parameter】

None

【description】

debug dhcpsnooping The command enables the debugging function of the dhcp-snooping module.

no debug dhcpsnooping The command disables the debugging function of the dhcp-snooping module.

By default, the debugging function is disabled.

【example】

#Turn on debugging for the dhcp-snooping module

Switch#configure terminal

Switch(config)#debug dhcpsnooping

Chapter 49 DHCP option82

49.1 dhcp option82 configuration command

49.1.1 dhcp-option82

【command】

dhcp-option82

no dhcp-option82

【config-mode】

Global/VLAN/port configuration mode

【parameter】

None

【description】

dhcp-option82: The command is used to enable the dhcp option82 function.

no dhcp-option82: Command to disable the dhcp option82 function.

By default, the dhcp option82 function is disabled in global and vlan configuration modes. The dhcp option82 function is enabled in port configuration mode.

Enabling the dhcp option82 option will make it possible to carry the option82 option in dhcp messages.

The function must be enabled in both global and port configuration mode or in both global and vlan configuration mode to take effect.

When vlan and port configuration mode are both enabled, the vlan-related configuration takes precedence.

【example】

#Global enablement of dhcp option82 function.

Switch#configure terminal

Switch(config)#dhcp-option82

49.1.2 dhcp-option82 format

【command】

dhcp-option82 format { normal | user-defined | verbose }

no dhcp-option82 format

【config-mode】

global configuration mode

【parameter】

Normal: Indicates that option82 is populated with MAC addresses.

user-defined: Indicates that option82 is populated with user-configured content.

Verbose: Indicates that option82 is populated with node identifiers.

【description】

dhcp-option82 format { normal | user-defined | verbose }The command is used to configure the fill format of the Option82 option content.

no dhcp-option82 format Command to restore the default condition.

By default, the content of the Option82 option uses the normal format, i.e. filled MAC addresses.

Notes:

To use the user-defined fill format, the contents of the Remote ID and Circuit ID must be configured.

【example】

#Configure Option82 option content as custom.

Switch#configure terminal

Switch(config)#dhcp-option82 format user-defined

49.1.3 dhcp-option82 format verbose node-identifier

【command】

dhcp-option82 format verbose node-identifier { hostname | mac | user-defined *node-value* **}**

no dhcp-option82 format verbose node-identifier

【config-mode】

Global configuration mode

【parameter】

mac: Indicates that option82 is populated with the system mac.

hostname: Indicates that option82 is populated with the system name.

user-defined: Represents option82 option content filled with user-configured node-value.

node-value: Node identifier content, string format, maximum length 60 characters.

【description】

dhcp-option82 format verbose node-identifier Command to configure verbose fill content.

no dhcp-option82 format verbose node-identifier Command to restore the default configuration.

By default, the verbose fill is mac.

【example】

#Configure the verbose fill to hostname.

Switch#configure terminal

Switch(config)#dhcp-option82 format verbose node-identifier hostname

49.1.4 dhcp-option82 information format

【command】

dhcp-option82 information format { ascii | hex }

no dhcp-option82 information format

【config-mode】

Global configuration mode

【parameter】

ascii: Represents information in ASCII format.

hex: Represents information in hex format.

【description】

dhcp-option82 information format Command to configure the Option82 message format.

no dhcp-option82 information format Command to restore the default configuration.

By default, the message format uses hex.

【example】

#Configure Option82 message format to ascii.

Switch#configure terminal

Switch(config)#dhcp-option82 information format ascii

49.1.5 dhcp-option82 circuit-id

【command】

dhcp-option82 circuit-id user-defined *circuit-value*

no dhcp-option82 circuit-id user-defined

【config-mode】

Port/VLAN configuration mode

【parameter】

circuit-value: circuit-id information, in the range of 1-128 characters.

【description】

dhcp-option82 circuit-id The command is used to configure the content of the Circuit ID in the Option82 option.

no dhcp-option82 circuit-id Command to delete circuit-id configuration.

By default, the Circuit ID content of the Option82 option is empty.

【example】

#Configure the content of the Circuit ID in the Option82 option under port 0/0/1 to test.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#dhcp-option82 circuit-id user-defined test

49.1.6 dhcp-option82 remote-id

【command】

dhcp-option82 remote-id user-defined *remote-value*

no dhcp-option82 remote-id user-defined

【config-mode】

Port/VLAN configuration mode

【parameter】

remote-value: remote-id information, in the range of 1-128 characters.

【description】

dhcp-option82 remote-id The command is used to configure the content of the Remote ID in Option82.

no dhcp-option82 remote-id Command to delete the remote-id configuration.

By default, the Remote-ID content of the Option82 option is empty.

【example】

#Configure the Remote ID in the Option82 option on port 0/0/1 to test.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#dhcp-option82 remote-id user-defined test

49.1.7 dhcp-option82 strategy

【command】

dhcp-option82 strategy { drop | keep | replace }

【config-mode】

Port/VLAN configuration mode

【parameter】

drop: Represents dropping of DHCP messages carrying Option82 option.

keep: Represents direct forwarding of DHCP packets carrying the Option82 option.

replace: represents the replacement of the content of Option82 in the original message before forwarding.

【description】

dhcp-option82 strategy { drop | keep | replace } The command configures the processing policy for DHCP request messages that contain the Option82 option.

no dhcp-option82 strategy { drop | keep | replace } Command to restore the default configuration.

By default, the processing policy is replace, i.e. replace and forward.

【example】

#Configure the processing policy for DHCP request messages on port 0/0/1 that contain the Option82 option to keep.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#dhcp-option82 strategy keep

49.1.8 dhcp-option82 device-id

【command】

dhcp-option82 device-id

no dhcp-option82 device-id

【config-mode】

Global configuration mode

【parameter】

None

【description】

dhcp-option82 device-id Command to enable the carry device-id function.

no dhcp-option82 device-id Command to restore the default configuration.

By default, no device-id information is carried, and this feature is only available for devices that support stacking.

【example】

#Enable carry device-id function.

Switch#configure terminal

Switch(config)#dhcp-option82 device-id

49.2 dhcp option82 monitor command

49.2.1 show dhcp-option82 interface

【command】

show dhcp-option82 interface [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, based on the physical port of the switch.

【description】

show dhcp-option82 interface command to view the Option82 configuration of the port.

【example】

#Find out the dhcp-option82 configuration of the port.

Switch(config)#show dhcp-option82 interface ethernet 0/0/1

Global informations of dhcpv4 option82

Status : Enabled

Format : Normal

Information format : HEX

Node identifier: (use switch mac)

Port mode informations of dhcpv4 option82

Interface ethernet e0/0/1

Status : Enable

Strategy : Replace

Circuit ID User-defined : NULL

Remote ID User-defined : NULL

dhcp-option82 interface display field description

Field	Description
Status	Global function enable status: Enabled, Disabled
Format	Fill content format
Information format	Message format
Node identifier	Node identifier content
Status	Port enable function status: enable, disable
Strategy	Forwarding policy for DHCP request messages with Option82 option: replace, drop, keep

Circuit ID User-defined	Circuit ID content
Remote ID User-defined	Remote ID content

49.2.2 show dhcp-option82 vlan

【command】

show dhcp-option82 vlan [***vlan-id*** **]**

【config-mode】

arbitrary configuration mode

【parameter】

vlan-id: VLAN ID, in the range 1-4094.

【description】

show dhcp-option82 vlan Command to view the Option82 configuration of a VLAN.

【example】

#View the dhcp-option82 configuration for a VLAN.

Switch(config)#show dhcp-option82 vlan

Status : Disabled

Format : Normal

Information format : HEX

Node identifier: (use switch mac)

VLAN 1:

Strategy : Replace

Circuit ID user-defined : NULL

Remote ID user-defined : NULL

dhcp-option82 vlan display field description

Field	Description
Status	Global function enable status: Enabled, Disabled
Format	Fill content format
Information format	Message format
Strategy	Forwarding policy for DHCP request messages with Option82 option: replace, drop, keep
Circuit ID User-defined	Contents of the Circuit ID in Option82 option
Remote ID User-defined	The contents of the Remote ID in Option82 option

Chapter 50 DLF control

50.1 DLF control configuration commands

50.1.1 unknown-discard unicast

【command】

unknown-discard unicast

no unknown-discard unicast

【config-mode】

port configuration mode

【parameter】

None

【description】

unknown-discard unicast command enables the discard unknown unicast function.

no unknown-discard unicast Command restores default.

By default the function is off, i.e. unknown unicast messages are forwarded. When the function is turned on, the device discards unknown unicast messages.

【example】

#Enable drop unknown unicast messages under port 0/0/1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#unknown-discard unicast

50.1.2 unknown-discard multicast vlan

【command】

unknown-discard multicast vlan *vlan-id*

no unknown-discard multicast vlan *vlan-id*

【config-mode】

global configuration mode

【parameter】

vlan-id: VLAN number, value range 1-4094.

【description】

unknown-discard multicast vlan command enables dropping unknown multicast in VLAN.

no unknown-discard multicast vlan command restores default.

The vlan must exist before the function can be enabled.

By default, the disable function, i.e. forwarding unknown multicast messages for all vlan.

【example】

#Enable to discard unknown multicast packets for vlan 2.

Switch#configure terminal

Switch(config)#unknown-discard multicast vlan 2

50.2 Monitoring commands for DLF control

50.2.1 show unknown-discard ethernet

【command】

show unknown-discard ethernet *port-id*

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, based on the physical port of the switch.

【description】

show unknown-discard ethernet The command is used to view the unknown message discard status of a port.

【example】

#View the configuration of the unknown-discard on port 0/0/1.

Switch(config)#show unknown-discard ethernet 0/0/1

Port Discarding Unknown Unicast

e0/0/1 disable

unknown-discard ethernet display field description

Field	Description
Port	Port number
Discarding Unknown Unicast	Discard unknown unicast messages enable state

50.2.2 show unknown-discard vlan

【command】

show unknown-discard vlan *vlan-id*

【config-mode】

arbitrary configuration mode

【parameter】

None

【description】

show unknown-discard vlan Command to view the status of discarded VLAN unknown multicast packets.

【example】

#Check the discard vlan 1 unknown multicast message configuration.

Switch(config)#show unknown-discard vlan 1

VLAN Discarding Unknown Multicast

1 disable

unknown-discard ethernet description of the display field

Field	Description
VLAN	vlan number
Discarding Unknown Unicast	Discard unknown multicast messages enable state

Chapter 51 SLF control

51.1 SLF control configuration command

51.1.1 unknown-discard src-mac

【command】

unknown-discard src-mac

no unknown-discard src-mac

【config-mode】

port configuration mode

【parameter】

None

【description】

unknown-discard src-mac The command enables the discard source unknown packet function.

no unknown-discard src-mac The command is used to disable the discard source unknown packet function.

By default, the enablement function, i.e. forwarding of source unknown messages, is cancelled.

【example】

#Enable drop source unknown packets on port 0/0/1.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#unknown-discard src-mac

51.2 Monitoring commands for SLF control

51.2.1 show unknown-discard src-mac

【command】

show unknown-discard src-mac [ethernet *port-id* **]**

【config-mode】

arbitrary configuration mode

【parameter】

port-id: Port number, based on the physical port of the switch.

【description】

show unknown-discard src-mac The command is used to view the discard source unknown message configuration.

【example】

check the configuration of port 0/0/1 to discard source unknown packets.

Switch#configure terminal

Switch(config)#show unknown-discard src-mac ethernet 0/0/1

Port Srcmac unknown discard status

0/0/1 enable

unknown-discard src-mac display field description

Field	Description
Port	Port number
Srcmac unknown discard status	Enabling status: disable, enable

Chapter 52 ErrorDisable

52.1 ErrorDisable configuration command

52.1.1 errdisable detect cause

【command】

errdisable detect cause { all | bpdu-guard | dhcp-snooping | loopback | port-security | storm-control }

no errdisable detect cause { all | bpdu-guard | dhcp-snooping | loopback | port-security | storm-control }

【config-mode】

global configuration mode

【parameter】

bpdu-guard: Represents the bpdu guard function in STP.

dhcp-snooping: Indicates the DHCP Snooping function, which is not actually supported, only the command is reserved.

loopback: Indicates the loopback detection function loopback detection.

port-security: Indicates the port security function.

storm-control: Indicates storm suppression function.

all: The command used to enable functions represents all the functions listed above.

【description】

errdisable detect cause Commands for enabling functions.

no errdisable detect cause Commands for canceling functions.

The command is used to cancel functions. By default, all functions are enabled.

note :

After the port is turned off by the Error Disabled function, it can be immediately restored through shutdown or no shutdown.

【example】

#Enable the ErrorDisabled function of bpdu guard.

Switch#configure terminal

Switch(config)#errdisable detect cause bpdu-guard

52.1.2 errdisable recovery cause

【command】

errdisable recovery cause { all | bpdu-guard | dhcp-snooping | loopback | port-security | storm-control }

no errdisable recovery cause { all | bpdu-guard | dhcp-snooping | loopback | port-security | storm-control }

【config-mode】

global configuration mode

【parameter】

bpdu-guard: Representing the bpdu-guard function in stp.

dhcp-snooping: Represents the DHCP Snooping feature, which is not actually supported, only the command is reserved.

Loopback: Represents loopback detection function loopback-detection.

port-security: Represents port security features.

storm-control: Represents the storm suppression function.

all: Represents all the functions listed above.

【description】

errdisable recovery cause Command to enable the automatic recovery function.

no errdisable recovery cause Command to cancel the automatic recovery function.

By default, the automatic recovery function is enabled.

note :

The time for automatic recovery can be set by configuring the command errdisable recovery interval.

【example】

#Enables the bpdu-guard function to automatically resume after the ErrorDisabled state.

Switch#configure terminal

Switch(config)#errdisable recovery cause bpdu-guard

52.1.3 errdisable recovery interval

【command】

errdisable recovery interval *interval-value*

no errdisable recovery interval

【config-mode】

global configuration mode

【parameter】

interval-value: Automatic recovery time, in the range of 10-10000, default value 300, in seconds.

【description】

errdisable recovery interval The command is used to configure the time for automatic state recovery.

no errdisable recovery interval Command to restore the default value.

By default, the automatic recovery time is 300 seconds.

【example】

#Set the automatic recovery time to 60 seconds.

Switch#configure terminal

Switch(config)#errdisable recovery interval 60

52.2 ErrorDisable manages monitoring and debugging commands

52.2.1 show errdisable

【command】

show errdisable

【config-mode】

any command mode

【parameter】

None

【description】

The show errdisable command is used to view the ErrorDisabled configuration and operational information.

【example】

#Find out about ErrorDisabled configuration and operational information.

Switch(config)#show errdisable

show err-disable information:

detect cause: loopback bpdu-guard

recovery cause: all

recovery interval time: 10000s

Port	Shutdowned	Cause	Recovery(s)
e0/0/1	FALSE	N/A	N/A
e0/0/2	FALSE	N/A	N/A
e0/0/3	FALSE	N/A	N/A
e0/0/4	FALSE	N/A	N/A

……

show errdisable display field description

Field	Description

Detect cause	List of functions enabled for detection
Recovery cause	List of features that enable automatic recovery
Recovery interval time	Automatic recovery time
Port	Port Number
Shutdowned	Detection status
Cause	Reasons for testing status
Recovery	Automatic recovery of remaining time

Chapter 53 ERPS

53.1 ERPS configuration command

53.1.1 erps

【Command】

erps

no erps

【Config-mode】

Global config-mode

【Parameter】

None

【Description】

The **erps** command is used to enable the erps function.

The **no erps** command is used to restore the default situation.

By default, the ERPS is in an off state.

【example】

#Enable ERPS function。

switch#configure terminal

switch(config)#erps

53.1.2 erps instance

【Command】

erps instance *instance-id*

no erps instance [*instance-id*]

【Config-mode】

Global config-mode

【Parameter】

instance-id: instance-id, Range 0-15.

【Description】

The **erps instance** command is used to create an ERPS instance and enter ERPS config-mode.

The **no erps instance** command is used to delete an ERPS instance that has been created.

By default, the device did not create an ERPS instance.

【Example】

#Create ERPS instance 0 and enter ERPS config-mode.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#

53.1.3 control-vlan

【Command】

control-vlan *vlan-id*

no control-vlan

【Config-mode】

ERPS config-mode

【Parameter】

vlan-id: Control vlan id for the ERPS instance,Range 1-4094.

【Description】

The **control-vlan** command is used to configure the control vlan for the ERPS instance.

The **no control-vlan** command removes the control vlan for the ERPS instance.

By default, the device ERPS instance is not configured with a control vlan.

Control vlan is required for the uncreated vlan id.

In the ERPS ring, the control VLAN is only used to deliver ERPS protocol packet and not to forward user service messages, thus improving the security of the ERPS protocol.

Instructions

All devices in the same ERPS ring must be configured with the same control VLAN.

If you need to delete a configured control VLAN, you must first de-enable the ring in ERPS config-mode before configuring a new control VLAN.

The control VLAN is a private VLAN for the ERPS and must be guaranteed not to be shared with other functions.

The control VLAN cannot be modified after starting the ERPS protocol on the ring.

Different ERPS rings cannot use the same ID for the control VLAN.

【example】

#Configure control vlan 100

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#control-vlan 100

53.1.4 guard-timer

【Command】

guard-timer *timer-value*

no guard-timer

【Config- Mode】

ERPS config-modes

【Parameters】

timer-value: guard timer timer value,The range is 10-2000 milliseconds, the default value is 500.

【Description】

The **guard-timer** command is used to configure the guard timer timer of the ERPS ring.

The **no guard-timer** command is used to restore the default value of the guard timer timer of the ERPS ring.

By default, the guard-timer timer is 500 milliseconds.

This timer is started when the port detects a link recovery and is used to prevent unnecessary shock to the network caused by residual original R-APS messages due to online forwarding delays. The interface no longer processes all R-APS messages until this timer times out. If a faulty R-APS message is received from another port after the timer timeout, the forwarding state of this port changes to Forwarding state.

【Examples】

#Configure the guard-timer timer to 200 milliseconds.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#guard-timer 200

53.1.5 mel

【Command】

mel *level-value*

no mel

【Config-Mode】

ERPS config-mode

【Parameters】

level-value: Specifies the value of the MEL field in the ERPS protocol message, in the range of 0-7, with the default value of 0.

【Description】

The **mel** command is used to configure the value of the MEL field in ERPS protocol packets.

The **no mel** command is used to restore the default value of the MEL field in ERPS protocol packets.

By default, the value of the MEL field in ERPS protocol packets is 0.

ERPS instance under mel associated cfm level.

【Examples】

#Configure the MEL field value level to 7.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#mel 7

53.1.6 port0

【Command】

port0 {eth-trunk *eth-trunk-id* **| ethernet** *port-id* **} [neighbour | next-neighbour | owner]**

no port0

【Config-mode】

ERPS config-mode

【Parameters】

eth-trunk-id: Aggregate group id number, range 1-16.

port-id: Port number in the format of: device number/slot number/port number.

neighbour: Indicates that the port joining the ERPS ring is in the RPL neighbour role.

next-neighbour: Indicates that the port joining the ERPS ring is in the RPL next- neighbour role.

owner: Indicates that the port joining the ERPS ring is in the RPL owner role.

【Description】

The **port0** command is used to configure the first port of the ERPS ring and its role.

The **no port0** command is used to delete the first port of the ERPS ring.

By default, the first port of the ERPS ring is not configured.

When only the port is configured and no port role is configured, the role of the port defaults to **common**.

Instructions:

There are only a maximum of two ports on an ERPS ring.

Ports that join ERPS rings cannot enable Spanning Tree, LBD, or EAPS protocols.

Plus two port roles within an ERPS ring cannot be the same.

The port cannot be modified after starting the ERPS protocol on the ring.

The port that joins the ERPS ring cannot be an access port.

【Examples】

#Configure port 23 as the first port of erps and the role as owner.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#port0 ethernet 0/0/23 owner

53.1.7 port1

【Command】

port1 {eth-trunk *eth-trunk-id* **| ethernet** *port-id* **} [neighbour | next-neighbour | owner]**

no port1

【Config-mode】

ERPS config-mode

【Parameters】

eth-trunk-id: Aggregate group id number, range 1-16.

port-id: Port number in the format of: device number/slot number/port number.

neighbour: Specifies that the port joining the ERPS ring is an RPL neighbour role.

next-neighbour: Specifies that the port joining the ERPS ring is the RPL next- neighbour role.

owner: Specifies that the port joining the ERPS ring is the RPL owner role.

【Description】

The **port1** command is used to configure the second port of the ERPS ring and its role.

The **no port1** command is used to delete the second port of the ERPS ring.

By default, no ERPS ring second port is configured.

When only the port is configured and no port role is configured, the role of the port defaults to **common**.

Instructions

l Up to two ports on an ERPS ring

l Ports that join ERPS rings cannot enable Spanning Tree, LBD, or EAPS protocols.

l Plus two port roles within an ERPS ring cannot be the same.

l The port cannot be modified after starting the ERPS protocol on the ring.

【Examples】

#Configure port 23 as the second port of erps and the role as common.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#port1 ethernet 0/0/23

53.1.8 protected-instance

【Command】

protected-instance *instance-id-list*

no protected-instance

【Config-mode】

ERPS config-mode

【Parameter】

instance-id-list: The list of referenced protection instances. The list of instances can be represented as single or multiple

instances. The symbol "," is used to insert discontinuous instances, and "-" is used to insert continuous instances. The range of instances is from 0 to 15, and the length of the string that can be entered is from 1 to 64.

【Description】

The **protected-instance** command is used to configure the protection instance of an ERPS ring.

The **no protected-instance** command is used to remove the protection instance of an ERPS ring.

By default, no protection instance of ERPS ring is configured.

The configured protection instance is implemented by referencing the mstp instance, so you need to configure the mstp instance first.

【Examples】

#Configure the protection instance of the ERPS ring to 15.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#protected-instance 15

53.1.9 ring

【Command】

ring *ring-id*

ring 1

【Config-mode】

ERPS config-mode

【Parameter】

ring-id: ERPS ring id, range 1-239.

【Description】

The **ring** command is used to enable the ERPS ring id.

The **ring 1** command is used to restore the default configuration.

By default, when an ERPS ring is created, ring id 1 is automatically created.

Only one ring id can exist in the same ERPS instance, and the latest configuration overwrites the old one. The ring ids can be the same for different ERPS instances.

【Examples】

#Configure the ERPS ring id to 2.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#ring 2

53.1.10 ring level

【Command】

ring level { 0 | 1}

【Config-mode】

ERPS config-mode

【Parameter】

0: Indicates the primary ring, default configuration.

1: indicates the subring.

【Description】

The **ring level** command is used to configure the ERPS ring type.

By default, ERPS is the primary ring.

【Examples】

#Configure the ERPS ring type as the primary ring.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#ring level 0

53.1.11 ring enable

【Command】

ring {enable | disable }

【Config-mode】

ERPS config-mode

【Parameter】

None

【Description】

The **ring enable** command is used to enable the ERPS ring.

The **ring disable** command is used to de-enable the ERPS ring.

By default, the ERPS ring is de-enabled.

You need to configure control-vlan, port (port0, port1) and ERPS instance before you can enable ERPS ring.

【Examples】

#Enables the ERPS ring.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#ring enable

53.1.12 work-mode

【Command】

work-mode { non-revertive | revertive }

【Config-mode】

ERPS config-mode

【Parameter】

non-revertive: Indicates running non-revertive mode, if the faulty link is restored, the WTR Timer timer is not started and

the blocked link remains on the original faulty link and does not cut back to the RPL.

revertive: indicates running revertive mode, if the failed link recovers, after waiting for WTR time, it will block the RPL owner port again, i.e. the blocked link will cut back to the RPL. Default operation mode.

【Description】

The **work-mode** command is used to configure the ERPS ring to be in either non-revertive or revertive mode.

By default, the ERPS ring is in revertive mode.

【Examples】

#Configure the ERPS ring to be in **non-revertive** mode.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#work-mode non-revertive

53.1.13 wtr-timer

【Command】

wtr-timer *timer-value*

no wtr-timer

【Config-mode】

ERPS config-mode

【Parameter】

timer-value: Wait time value, the value range is 1-12 minutes, the default value is 5.

【Description】

The **wtr-timer** command is used to configure the wait time for ERPS ringback mode switching.

The **no wtr-time** command is used to restore the wait time for ERPS ringback cut mode switching to the default value.

By default, the ERPS ring wait time for revertive mode is 5 minutes.

【Examples】

#Configure the wait time for ERPS ring revertive mode to 3 minutes.

switch#configure terminal

switch(config)#erps instance 0

switch(config-erps-instnace-0)#wtr-timer 3

53.2 ERPS monitoring and debugging Command

53.2.1 show erps

【Command】

show erps

【Config-mode】

Arbitrary config-mode

【Parameter】

None

【Description】

The **show erps** command is used to view all ERPS ring details.

By default, the ERPS ring is off.

【Examples】

#View ERPS ring details.

switch(config)#show erps

ERPS state : enable

Instance Id : 0

Mel : 0

Work-mode : revertive

WTR Timer : 5 min

Guard Timer : 500 ms

Holdoff Timer : 0 s

Ring 1 info :

Control vlan : 100

Status : enable

Protected-instance : 0

Role : Owner

Sub-ring : No

Stm : Pending

---

port portId role state nodeId BPR

---

port0 e0/0/2 Owner Blocking 00:00:00:00:00:00 0

port1 e0/0/4 Common Forwarding 00:00:00:00:00:00 0

Total 1 ring(s).

show erps .Display field description

Fields	Description
ERPS state	Global ERPS Status: enable、disable
Instance Id	ERPS Instance id
Mel	MD level value of R-APS protocol message

Work-mode	Work Mode: rvertive、non-revertive
WTR Timer	Working mode switching waiting time
Guard Timer	The amount of time after fault recovery that RAPS messages are not processed.
Holdoff Timer	Fault delay reporting time, the default value is 0, do not support to modify
Ring 1 info	Ring id
Control vlan	Control vlan id
Status	ERPS ring status :enable、disable
Protected-instance	Reference protection instance id
Role	Node Roles: Owner Node, Neighbor Node, Next-Neighbour Node, Common Node
Sub-ring	Is it a sub-ring: Yes、No
Stm	Node Status: init、idle、pending、protection
port	Port of ERPS ring: port0、 port1
portId	Port number
role	Port Roles: owner、neighbor、next-neighbour、common
state	Port Status: blocking、forwarding

nodeId	On the Owner node: the Node ID is: 00:00:00:00:00:00 On other nodes: por0 and port1 both have Node ID as owner MAC.
BPR	The PBR information on the Owner node is displayed as 0. The PBR information on other nodes is displayed as: the number corresponding to the Owner port (PBR=1 if port1 is the Owner port; PBR=0 if port0 is the Owner port;)

53.2.2 show erps statistics

【Command】

show erps statistics

【Config-mode】

Arbitrary config-mode

【Parameter】

None

【Description】

The **show erps statistics** command is used to view the statistics of all rings.

【Examples】

#View the statistics of the ERPS ring.

switch(config)#show erps statistics

Show packets input/output statistic information

Instance 0 Ring 1 :

port0 e0/0/2:

Input: nr 0, sf 0, nrrb 0

Output: nr 27, sf 8, nrrb 15

port1 e0/0/4:

Input: nr 0, sf 1, nrrb 0

Output: nr 27, sf 20, nrrb 15

show erps statistics Display field description

Field	Description
Port0	First port
input	Statistics of received nr, sf, nrrb packets
output	Statistics of outgoing nr,sf,nrrb packets
Port1	Second port

53.2.3 show erps instance

【Command】

show erps instance *instance-id* **[statistics]**

【Config-mode】

Arbitrary config-mode

【Parameter】

instance-id: ERPS instance id, range 0-15.

【Description】

The **show erps instance** command is used to view the details of the specified instance of ERPS.

The **show erps instance id statistics** command is used to view the statistics of the specified instance of ERPS.

【Examples】

#View the details of the specified ERPS ring.

switch(config)#show erps instance 0

ERPS state : enable

Instance Id : 0

Mel : 0

Work-mode : revertive

WTR Timer : 5 min

Guard Timer : 500 ms

Holdoff Timer : 0 s

Ring 1 info :

Control vlan : 100

Status : enable

Protected-instance : 0

Role : Owner

Sub-ring : No

Stm : Pending

---

port portId role state nodeId BPR

---

port0 e0/0/2 Owner Blocking 00:00:00:00:00:00 0

port1 e0/0/4 Common Forwarding 00:00:00:00:00:00 0

Total 1 ring(s).

show erps instance 0 .Display field description

Field	Description
ERPS state	Global ERPS Status: enable、disable
Instance Id	Specify ERPS instance id
Mel	MD level value of R-APS protocol packets
Work-mode	ERPS Working Mode: rvertive、non-revertive
WTR Timer	Working mode switching waiting time
Guard Timer	Time to not process RAPS packets after failure recovery
Holdoff Timer	Fault delay reporting time, the default value is 0, do not support to modify
Ring 1 info	Ring id
Control vlan	Control vlan id
Status	ERPS ring status :enable、disable
Protected-instance	Reference protection instance id
Role	Node Roles: owner、neighbor、next-neighbour、common
Sub-ring	ERPS ring type: Yes: Sub-ring No: Main ring

Stm	Node Status: init、idle、pending、protection
port	Port of ERPS ring: port0、 port1
portId	Port number
role	Port Role: owner、neighbor、next-neighbour、common
state	Port Status: blocking、forwarding
nodeId	On the Owner node: the Node ID is: 00:00:00:00:00:00 On other nodes: por0 and port1 both have Node ID as owner MAC.
BPR	The PBR information on the Owner node is displayed as 0. The PBR information on other nodes is displayed as: the number corresponding to the Owner port (PBR=1 if port1 is the Owner port; PBR=0 if port0 is the Owner port).

#View the statistics for the specified instance of ERPS.

switch(config)#show erps instance 0 statistics

Show packets input/output statistic information

Instance 0 Ring 1 :

port0 e0/0/2:

Input: nr 0, sf 0, nrrb 0

Output: nr 27, sf 8, nrrb 15

port1 e0/0/4:

Input: nr 0, sf 1, nrrb 0

Output: nr 27, sf 20, nrrb 15

show erps instance 0 statistics .Display field description

Field	Description
Port0	First port
input	Statistics of received nr,sf,nrrb packets
output	Statistics of outgoing nr,sf,nrrb packets
Port1	Second port

53.2.4 show erps control-vlan

【Command】

show erps control-vlan [*vlan-id* **]**

【Config-mode】

Arbitrary config-mode

【Parameter】

vlan-id: vlan id, range 1-4094.

【Description】

The **show erps control-vlan** command is used to view all ring control vlan of ERPS.

If vlan id is specified, only the specified control vlan is viewed.

【Examples】

#View the ERPS ring detail control vlan.

switch(config)#show erps control-vlan

VLAN name : ERPS instance 0 ring 1 control-vlan 10

VLAN ID : 10

VLAN status : ERPS used only

VLAN member : e0/0/2,e0/0/4.

Static tagged ports : e0/0/2,e0/0/4.

Static untagged ports :

VLAN name : ERPS instance 1 ring 1 control-vlan 20

VLAN ID : 20

VLAN status : ERPS used only

VLAN member :

Static tagged ports :

Static untagged ports :

Total entries: 2 vlan.

show erps control-vlan Display field description

Field	Description
VLAN name	Vlan name, fixed:: ERPS instance instance-id ring ring-id control-vlan vlan-id
VLAN ID	vlan id
VLAN status	Vlan state, fixed: ERPS used only
VLAN member	Members of the vlan for port 1 and port 2 of the ERPS ring
Static tagged ports	tagged members list
Static untagged ports	untagged members list

53.2.5 clear erps statistics

【Command】

clear erps { statistics | instance *instance-id* **statistics }**

【Config-mode】

Global config-mode

【Parameter】

instance-id: ERPS ring id, range 0-15.

【Description】

The **clear erps statistics** command is used to clear statistics on all ERPS rings.

If a ring is specified, the statistics on the specified ring are cleared.

【Examples】

#Clears statistics on all rings in ERPS.

switch(config)#clear erps statistics

53.2.6 debug erps

【Command】

debug erps

no debug erps

【Config-mode】

Global config-mode

【Parameter】

None

【Description】

The **debug erps** command opens all debugging information of ERPS.

The **no debug erps** command turns off all debugging information for ERPS.

By default, all debug switches in ERPS are off.

【Examples】

#Turn on all debugging information for ERPS

switch#configure terminal

switch(config)#debug erps

Chapter 54 VRRP

54.1 VRRP Configuration Command

54.1.1 vrrp vrid virtual-ip

【Command】

vrrp vrid *vrid-id* **virtual-ip** *ip-address*

no vrrp vrid *vrid-id* **[virtual-ip** *ip-address* **]**

【Config-mode】

VLAN interface config-mode

【Parameter】

vrid-id: VRRP group number, range 1-255.

ip-address: ip address, dotted decimal, format:x.x.x.x.

【Description】

The **vrrp vrid vrid-id virtual-ip** command is used to create a virtual group and configure the ip address.

The **no vrrp vrid vrid-id virtual-ip** command is used to delete the ip address of a virtual group.

The **no vrrp vrid vrid-id** command is used to delete all configurations of a virtual group.

By default, no virtual group exists. The maximum number of ip addresses supported for the same virtual group is 8.

Instructions

VRRP virtual ip address should be on the same segment as the VLAN interface address

Allows configuration of up to 255 backup groups and up to 8 IP addresses per backup group.

If the virtual group IP address is the same as the VLAN interface IP, the switch is said to be the address owner (IP Address Owner)

When specifying the first IP address to a backup group, the system creates this backup group, and when specifying a virtual IP address to this backup group later, the system simply adds this address to the list of virtual IP addresses for this backup group.

When the last virtual IP address in the backup group is deleted, this backup group will also be deleted at the same time.

That is, this backup group is no longer available on this interface, and all configurations of this backup group are no longer valid.

【Examples】

#Configure vlan interface 10 vrid 1 virtual ip address.

switch#configure terminal

switch(config)#interface vlan-interface 10

switch(config-if-vlanInterface-10)#vrrp vrid 1 virtual-ip 192.168.50.51

54.1.2 vrrp vrid advertise-interval

【Command】

vrrp vrid *vrid-id* **advertise-interval** *interval-value*

no vrrp vrid *vrid-id* **advertise-interval**

【Config-mode】

VLAN interface config-mode

【Parameter】

vrid-id: VRRP group number, the value range is 1-255.

interval-value: The sending period of the VRRP packet, in seconds, in the range 1-255, default 1.

【Description】

The **vrrp vrid vrid-id advertise-interval** command is used to configure the sending period of VRRP advertisement messages for the specified vrid.

The **no vrrp vrid vrid-id advertise-interval** command is used to restore the sending period of the notification message for the specified vrid to the default value.

By default, the sending period of VRRP advertisement messages is 1 second.

You need to configure the interface virtual ip first before you can configure the VRRP message sending period.

【Examples】

#Configure the VRRP message sending period for vlan interface 10 vrid 1 to be 3 seconds.

switch#configure terminal

switch(config)#interface vlan-interface 10

switch(config-if-vlanInterface-10)#vrrp vrid 1 advertise-interval 3

54.1.3 vrrp vrid preempt-mode

【Command】

vrrp vrid *vrid-id* **preempt-mode**

no vrrp vrid *vrid-id* **preempt-mode**

【Config-mode】

VLAN interface config-mode

【Parameter】

vrid-id: VRRP group number, range 1-255.

【Description】

The **vrrp vrid vrid-id preempt-mode** command is used to enable the preemption function for the specified vrid.

The **no vrrp vrid vrid-id preempt-mode** command is used to disable the preemption function of the specified vrid.

By default, the preemption function is enabled.You need to configure the interface virtual ip before you can configure the preemption function.

If the switch's virtual group disables preemption, the Master and Backup remain permanently unchanged and are not re-elected.

If the switch's virtual group enables the preemption feature, a notification message is sent to re-elect the Master when the priority of the Backup is higher than the priority of the Master.

【Examples】

#vlan interface 10 disables vrid 1 preemption

switch#configure terminal

switch(config)#interface vlan-interface 10

switch(config-if-vlanInterface-10)#no vrrp vrid 1 preempt-mode

54.1.4 vrrp vrid preempt-mode delay

【Command】

vrrp vrid *vrid-id* **preempt-mode delay** *delay-value*

【Config-mode】

VLAN interface config-mode

【Parameter】

vrid-id: VRRP group number, the value range is 1-255.

delay-value: Preemption delay time, in the range of 0-255, in seconds, default 0.

【Description】

The **vrrp vrid vrid-id preempt-mode delay** command is used to configure the preemption delay time.

By default, the preemption delay time is 0.

You need to configure the interface virtual ip before you can configure the preemption delay time.

The preemption delay time is required to enable the preemption function. The purpose of setting the delay time is that in a less stable network, if the Backup does not receive the message from the Master on time, it will become the Master (and the reason why the Backup does not receive the message is due to network blockage, not because the Master is not working properly). (not because the Master is not working properly), increasing the preemption delay can avoid frequent state transitions.

【Examples】

#Configure the preemption delay for vlan interface 10 vrid 1 to be 5 seconds.

switch#configure terminal

switch(config)#interface vlan-interface 10

switch(config-if-vlanInterface-10)#vrrp vrid 1 preempt-mode delay 5

54.1.5 vrrp vrid priority

【Command】

vrrp vrid *vrid-id* **priority** *priority -value*

no vrrp vrid *vrid-id* **priority**

【Config-mode】

VLAN Interface config-mode

【Parameter】

vrid-id: VRRP group number, range 1-255.

priority-value: The priority of VRRP, with a value range of 1-254 and a default of 100.

【Description】

The **vrrp vrid vrid-id priority** command is used to configure the priority of the specified vrid.

The **no vrrp vrid vrid-id priority** command is used to restore the priority to the default value.

By default, the VRRP priority is 100.

You need to configure the interface virtual ip before you can configure the VRRP priority.

A higher priority value indicates a higher priority.

The switches in a backup group determine their role in the backup group based on their priority. The switch with higher priority becomes the Master switch and the one with lower priority becomes the Backup switch.

【Examples】

#Configure vlan interface 10 vrid 1 priority to 150.

switch#configure terminal

switch(config)#interface vlan-interface 10

switch(config-if-vlanInterface-10)#vrrp vrid 1 priority 150

54.1.6 vrrp vrid track

【Command】

vrrp vrid *vrid-id* **track{ supervlan-interface** *supervlan-id* **| vlan-interface** *interfacevlan-id* **} [reduced** *priority -value* **]**

no vrrp vrid *vrid-id* **track {all | supervlan-interface** *supervlan-id* **| vlan-interface** *interfacevlan-id* **}**

【Config-mode】

VLAN interface config-mode

【Parameter】

vrid-id: VRRP group number, range 1-255.

supervlan-id: Super vlan interface id, range 1-128.

interfacevlan-id: Common vlan interface id, range 1-4094.

priority -value: Priority, value range is 1-254, default is 10.

【Description】

The **vrrp vrid** *vrid-id* **track** command is used to configure the monitoring interface of the specified vrid.

The **no vrrp vrid** *vrid-id* **track** command is used to remove the monitoring interface of the specified vrid.

By default, there is no monitoring interface. You need to configure the interface virtual ip before you can configure the detection interface of VRRP.

The VRRP track function monitors the uplink interface or uplink state and changes the priority of the interface according to the uplink state. When the monitored interface is down, the default action is to reduce the priority of its own interface by 10.

When the uplink fails and the hosts in the LAN cannot access the external network through the switch, the status of the monitored Track item is Down and the priority of the router is actively reduced by a certain value (the value can be configured). This makes other switches in the backup group have higher priority than this switch and become the master switch to ensure that the communication between the hosts in the LAN and the external network will not be interrupted.

【Examples】

#Configure vlan interface 10 vrid 1 to detect vlan interface 1.

switch#configure terminal

switch(config)#interface vlan-interface 10

switch(config-if-vlanInterface-10)#vrrp vrid 1 track vlan-interface 1

54.2 VRRP Monitoring and Commissioning command

54.2.1 show vrrp status

【Command】

show vrrp status [supervlan-interface *supervlan-id* **| vlan-interface** *interfacevlan-id* **]**

【Config-mode】

Arbitrary config-mode

【Parameter】

supervlan-id: super VLAN interface id, the range is 1-128.

interfacevlan-id: ordinary VLAN interface id, the value range is 1-4094.

【Description】

The **show vrrp status** command is used to view VRRP status information.

【Examples】

#View VRRP status information.

switch(config)#show vrrp status

Show informations of VRRP status

Virtual IP Ping: Enable

VLAN-IF10 | Virtual Router 1

State : Master

Virtual IP : 192.168.50.50 192.168.50.100

Virtual MAC : 00:00:5e:00:01:01

Master IP : 192.168.50.20

Primary IP : 192.168.50.20

Priority : 100

Preempt : YES

Delay Time (secs) : 0

Timer (secs) : 1

track interfaces:

Total entries:1

show vrrp status .Display field description

Field	Description
Virtual IP Ping	Ping virtual ip function: enable、disable
VLAN-IF10 | Virtual Router 1	The name of the interface where the VRRP group is located and the VRRP group number
State	Current Role: Master、Backup
Virtual IP	Virtual IP address
Virtual MAC	Virtual mac address
Master IP	Master device ip address
Primary IP	Master Virtual ID Address
Priority	Priority of VRRP
Preempt	Preemption function enable: YES、NO
Delay Time	Grabbing delay time
Timer	Period of sending announcement packets
track	Monitoring Interface

54.2.2 show vrrp statistics

【Command】

show vrrp statistics [supervlan-interface *supervlan-id* **| vlan-interface** *interfacevlan-id* **]**

【Config-mode】

Arbitrary config-mode

【Parameter】

supervlan-id: Super VLAN interface id, the range is 1-128.

interfacevlan-id: Common VLAN interface id, the value range is 1-4094.

【Description】

The **show vrrp statistics** command is used to view VRRP statistics.

【Examples】

#View VRRP Statistics.

switch(config)#show vrrp statistics

Show informations of VRRP statistics

Checksum errors : 0

Version errors : 0

Vrid errors : 0

VLAN-IF10 | Virtual Router 1

Transited to master : 1

Received advertisements : 0

Advertisement interval errors : 0

Failed to authentication check : 0

Received ip ttl errors : 0

Received packets with priority zero : 0

Send packets with priority zero : 0

Received invalid type packets : 0

Received unmatched address list packets : 0

Unknow authentication type packets : 0

Mismatched authentication type : 0

Packet lenth errors : 0

Total entries: 1

show vrrp statistics Display field description

Field	Description
Checksum errors	Check digit error packet
Version errors	Version error packet
Vrid errors	Vird error packet
VLAN-IF10 | Virtual Router 1	Interface name and VRRP group number where the VRRP group is located
Received advertisements	Received notification packet
Advertisement interval errors	Notification interval error packet
Failed to authentication check	Authentication failure packet
Received ip ttl errors	Received ip ttl error packet
Received packets with priority zero	Receive a priority 0 packet
Send packets with priority zero	Send a priority 0 packet
Received invalid type packets	Receive a packet with an invalid message type

Received unmatched address list packets	Received a packet that does not match the id address list
Unknow authentication type packets	Packets with unknown authentication type
Mismatched authentication type	Packets with mismatched authentication types
Packet lenth errors	Packets with wrong message length

54.2.3 debug vrrp

【Command】

debug vrrp

no debug vrrp

【Config-mode】

Global config-mode

【Parameter】

None

【Description】

The **debug vrrp** command turns on VRRP debugging information.

The **no debug vrrp** command turns off VRRP debug information.

By default, the VRRP debug switch is off.

【Examples】

#Turn on VRRP debugging information

switch#configure terminal

switch(config)#debug vrrp

Chapter 55 Network Testing & Troubleshooting

55.1 Network testing and troubleshooting commands

55.1.1 ping

【Command】

ping [-s *ip-address*] **[-c** *number*] **[-i** *ttl-value*]**[-l** *length-value*] **[-t** *timeout-value*] *ip-address*

【Config-mode】

Arbitrary Config-mode

【Parameter】

-s: Indicates that the source IP address is modified.

-c: indicates modify the number of messages.

-i: indicates modify the TTL.

-l: indicates modify the message data length.

-t: indicates modify the timeout time.

ip-address: ip address in dotted decimal format: x.x.x.x.

number: the number of messages, the value range is 1-2147483647, default 5.

ttl-value: ttl value, range is 1-255, default is 64.

length-value: length of data in bytes, in the range of 0-4064, default 58.

timeout-value: wait timeout time, in seconds, range is 1-60, default is 1.

【Description】

The **ping** command is used to check whether the specified destination address is reachable.

During the execution of the ping command, type the key combination < Ctrl+C > to stop the ping operation.

【Example】

#ping 1.1.1.1,specify to send 6 times

Switch#configure terminal

Switch(config)#ping -c 6 1.1.1.1

PING 192.168.1.111 (192.168.1.111) 56(84) bytes of data.

64 bytes from 192.168.1.111: icmp_seq=1 ttl=64 time < 1ms

64 bytes from 192.168.1.111: icmp_seq=2 ttl=64 time < 1ms

64 bytes from 192.168.1.111: icmp_seq=3 ttl=64 time < 1ms

64 bytes from 192.168.1.111: icmp_seq=4 ttl=64 time < 1ms

64 bytes from 192.168.1.111: icmp_seq=5 ttl=64 time < 1ms

64 bytes from 192.168.1.111: icmp_seq=6 ttl=64 time < 1ms

--- 192.168.1.111 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 5000ms

rtt min/avg/max/mdev = 0/0/0/0 ms

55.1.2 ping6

【Command】

ping6 [-h *hop-value* **][-s** *length-value* **][-c** *number* **][-a** *ipv6-address* **][-w** *timeout-value* **] [-t]** *ipv6-address*

【Config-mode】

Arbitrary config-mode

【Parameter】

-h: ndicates modify the number of hops.

-s: indicates modify the length of the message data.

-c: indicates modify the number of messages.

-a: indicates modify source IP address.

-w: indicates modify the timeout time.

-t: Indicates that the number of messages is infinite and the priority is higher than -c.

hop-value: the number of hops, the range is 1-255, the default is 5.

len-value: data length in bytes, the range is 20-8100, the default is 56.

count-value: the number of packets sent, in the range of 1 to 2147483647, default 5.

ipv6-address: IPv6 address, in bold hexadecimal format: x:x:x:x:x:x.

timeout-value: timeout time, in seconds, in the range of 1-60, default 1.

【Description】

The **ping6** command is used to check whether the specified destination address is reachable.

During the execution of the ping6 command, type the key combination < Ctrl+C > to stop the ping6 operation.

【Example】

#ping6 2001::1, Send 2 packets.

Switch#configure terminal

Switch(config)#ping6 -c 2 2001::1

PING 2001::1(2001::1) 56 data bytes

64 bytes from 2001::1: icmp_seq=1 ttl=128 time=10.0 ms

64 bytes from 2001::1: icmp_seq=2 ttl=128 time < 1ms

--- 2001::1 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1010ms

rtt min/avg/max/mdev = 0/5/10/5 ms

55.1.3 tracert

【Command】

tracert [**-c** | **-u** [**-p** *udp-port*]] [**-s** *ip-address*] [**-f** *ttl-value*] [**-h** *hop-value*] [**-w** *timeout-value*] *ip-address*

【Config-mode】

Arbitrary config-mode

【Parameter】

-c: means use icmp packet probing.

-u: means use udp packet probing.

-p: means modify udp port number.

-s: means modify the source IP address.

-f: means modify ttl.

-h: Indicates modify the number of probes.

-w: means modify the timeout time.

ip-address: IP address in dotted decimal format: x.x.x.x.

ttl-value: the starting ttl value of the probe message, the value range is 1-255, the default is 1.

hop-value: the maximum number of probes, the value range is 1-255, the default 30.

timeout-value: timeout time in seconds, the value range is 1-60.

udp-port: UDP port number, the value range is 1-65535.

【Description】

The **tracert** command is used to view the gateway through which the datagram passes from the source to the destination.

During the execution of the tracert command, type the key combination < Ctrl+C > to stop the tracert operation.

【Example】

#View the gateway through which 192.168.1.111 passes.

Switch#configure terminal

Switch(config)#tracert 192.168.1.111

traceroute to 192.168.1.111 (192.168.1.111), 30 hops max, 60 byte packets

1 192.168.1.111 (192.168.1.111) 10.000 ms 10.000 ms 0.000 ms

55.1.4 tracert6

【Command】

tracert ipv6 [-c *num-per-hop* **] [-h** *hop-value***] [-w** *timeout-value* **]** *ipv6-address*

【Config-mode】

Arbitrary config-mode

【Parameters】

-c: Indicates that the number of probes per hop is modified.

-h: indicates modify the t tl of the probe message.

-w: means modify the timeout time.

Ipv6-address: IP address in bold hexadecimal format, e.g. 2000::1.

num-per-hop: the number of probes, the value range is 1-10, the default is 3.

hop-value: the starting ttl value of the probe message, the range is 1-255, the default is 30.

timeout-value: timeout time, the value range is 1-60, the default is 5, the unit of seconds.

【Description】

The **tracert ipv6** command is used to view the network through which a datagram travels from the source to the destination.

During the execution of the **tracert ipv6** command, type the key combination < Ctrl+C > to interrupt the probe

【Example】

#View to the network through which 2000::80 passes.

Switch#configure terminal

Switch(config)#tracert ipv6 -h 20 2000::80

traceroute to 2000::80 (2000::80), 20 hops max, 80 byte packets

1 2000::1 (2000::1) 2978.000 ms !H 2978.000 ms !H 2978.000 ms !H

Chapter 56 SNMP

56.1 SNMP configuration commands

56.1.1 snmp-server { enable | disable }

【Command】

snmp-server { enable | disable}

【Config-mode】

Global config-mode

【Parameter】

enable: Indicates that the snmp-server function is enabled.

disable: Indicates that the snmp-server function is de-enabled.

【Description】

The **snmp-server enable** command is used to enable the snmp-server function.

The **snmp-server disable** command is used to disable the enable function.

By default, the function is disabled.

【Example】

#Enable the snmp-server function.

Switch#configure terminal

Switch(config)#snmp-server enable

56.1.2 snmp-server contact

【Command】

snmp-server contact *contact-value*

no snmp-server contact

【Config-mode】

Global Config-mode

【Parameter】

contact: specify the contact information for the facility manager.

contact-value: contact value, up to 255 characters, default: http://.

【Description】

The **snmp-server contact** command is used to configure the contact information of the device administrator.

The **no snmp-server contact** command is used to restore to the default value.

By default, the contact information of the device administrator is http://.

【Example】

#Configure the device manager's contact information as test.

Switch#configure terminal

Switch(config)#snmp-server contact test

56.1.3 snmp-server location

【Command】

snmp-server location *location-value*

no snmp-server location

【Config-mode】

Global Config-mode

【Parameters】

location: specify how to contact the location of the device.

location-value: Takes a value up to 255 characters in length.

【Description】

The **snmp-server location** command is used to configure the location where the device is placed.

The **no snmp-server location** command is used to restore to the default information.

By default, the location information is sample sysLocation factory default.

The **snmp-server contact** and **location** commands are used to enable the network management workstation to read out the information about the device manager and the specific location of the device, so as to facilitate the management of the device.

【Example】

#Configure the device placement to aaaaaa.

Switch#configure terminal

Switch(config)#snmp-server location aaaaa

56.1.4 snmp-server name

【Command】

snmp-server name *name-value*

no snmp-server name

【Config-mode】

Global Config-mode

【Parameter】

name: Specifies the system name of the device.

name-value: The system name takes the value and is no more than 255 characters long.

【Description】

The **snmp-server name** command modifies the system name of the device.

The **no snmp-server name** command is used to restore to the default information.

By default, the format is :Switch + product name.

【Example】

#Configure name as test.

Switch#configure terminal

Switch(config)#snmp-server name test

56.1.5 snmp-server community

【Command】

snmp-server community *community-name* **{ rw | ro } { permit | deny } [view** *view-name* **]**

no snmp-server community *community-name*

【Config-mode】

Global Config-mode

【Parameter】

community-name: the name of the group, maximum length 32 characters.

rw: Specify that the operation permission of the community name is read-write.

ro: Specify that the operation privilege of the community name is read-only.

view-name: the name of the view, maximum length is 32 characters.

【Description】

The **snmp-server community** command is used to configure the group name of the SNMP agent.

The **no snmp-server community** command is used to delete the group name of the SNMP agent.

Usually the community name and the community name configured on the network management workstation should be the same, otherwise the network management workstation cannot perform any operation on the device.

view is used to specify the view range for the group, without view means use the default view ISO.

【Example】

#Configure the group name of the SNMP agent as public, with read and write permissions.

Switch#configure terminal

Switch(config)#snmp-server community public rw permit

56.1.6 snmp-server view

【Command】

snmp-server view *view-name oid-value* **{ exclude | include}**

no snmp-server view *view-name [oid-value]*

【Config-mode】

Global Config-mode

【Parameter】

view-name: Specify the view name, the length of the string is not greater than 32 characters.

oid-value:the OID of the MIB subtree to which the view corresponds.

exclude: indicates that the scope of the view is all the objects outside the node.

include: indicates that the scope of the view is all objects within the node.

【Description】

The **snmp-server view** command is used to configure the view of the SNMP agent.

The **no snmp-server view** command is used to remove the view of the SNMP agent.

By default, views iso, system and internet exist. where the subtree of iso is 1 and type is include; the subtree of system is 1.3.6.1.2.1 and type is include; the subtree of internet is 1.3.6 and type is include.

【Example】

#Create include view MIB1, node subtree 1.3.6.1.2.1.

Switch#configure terminal

Switch(config)#snmp-server view mib1 1.3.6.1.2.1 include

56.1.7 snmp-server group

【Command】

snmp-server group *group-name* **3 { noauthpriv | auth | priv } read** *view-name* **write** *view-name* **notify** *view-name* **[context** *context-name* **]**

no snmp-server group *group-name* **3 { noauthpriv | auth | priv } [context** *context-name***]**

【config-mode】

Global Config-mode

【Parameter】

group-name: group name, in the form of a string, no longer than 32 characters.

3: indicates SNMPv3.

noauthpriv: Indicates that the security level of the group is no authentication without encryption.

auth: indicates that the security level of the group is authentication but not encryption.

priv: Indicates that the security level of the group is both authenticated and encrypted.

view-name: the name of the view, no longer than 32 characters, in string form.

context-name: context environment, no more than 32 characters long, in string form.

【Description】

The **snmp-server group** command is used to configure SNMPv3 group-related information.

The **no snmp-server group** command is used to delete the specified SNMPv3 group information.

By default, the device does not configure SNMPv3 group-related information.

In SNMPv3, a group name, security information, and a message type (read operation, write operation, or announcement) are mapped to a MIB view. Given a MIB view, it is possible to determine whether a managed object is allowed to be accessed, while several SNMPv3 users can be associated to the group. The group setting enhances the access control strength of SNMPv3.

【Example】

#Configure a group with the name group1, the security level is unauthenticated and unencrypted, and the read/write notification view is ISO.

Switch#configure terminal

Switch(config)#snmp-server group group1 3 noauthpriv read iso write iso notify iso

56.1.8 snmp-server user

【Command】

snmp-server user *user-name group-name*

snmp-server user *user-name group-name* **auth { md5 | sha }{ auth-password | auth-key }** *auth-value*

snmp-server user *user-name group-name* **auth { md5 | sha }{ auth-password | auth-key }** *auth-value* **priv {aes | des }**

{ priv-password | priv-key } *priv-value*

no snmp-server user *user-name*

【Config-mode】

Global Config-mode

【Parameter】

user-name: user name, in the form of a string, no longer than 32 characters.

group-name: group name, in the form of a string, not longer than 32 characters.

port-number-value: the udp port number of the specified remote user, in the form of an integer, in the range of 1-65535.

auth: The security level is authentication.

md5: Use MD5 hash function for authentication.

sha: use SHA hash function for authentication.

priv aes: encrypted using the aes algorithm.

priv des: Encryption using the des algorithm.

auth-password *auth-value*: authentication password, in string form, length 8-32 characters.

auth-key *auth-value*: MD5 authentication key, combined with hash function to generate authentication code to achieve the authentication function, MD5 authentication string length of 32 characters, SHA authentication string length of 40 characters.

priv-password *priv-value*: encrypted password, string form, length 8~32 characters.

priv-key *priv-value*: encryption key, combined with the hash function to generate the authentication code to achieve the authentication function, in the form of a string, length 32 characters.

【Description】

The snmp-server user user-name group-name command is used to configure local users with the security level of noauthpriv.

The snmp-server user user-name group-name auth { md5 | sha }{ auth-password | auth-key } auth-value commandis used to configure local users with security level auth.

The snmp-server user user-name group-name auth { md5 | sha }{ auth-password | auth-key } auth-value priv {aes | des } { priv-password | priv-key } priv-value commandis used to configure local users with the security level authpriv.

The no snmp-server user command is used to remove the local user configuration.

Three users exist by default: initialnone, initialmd5, and initialsha.

Use this Command to create a user in an SNMP group and configure the group to which the user belongs and the authentication method so that the Agent can be accessed only if the user and key information of the NMS is the same as the user information configured on the device. this Command is only used in SNMP v3. SNMPv1 and SNMP v2c do not have the concept of SNMP combinations and users. Instead, the Community is used.

Notes:

The security level of the user must be the same as the security level of the group. If the security level of the user is NoauthPriv, the security level of the group to which the user belongs must also be NoauthPriv, otherwise the user is invalid and cannot access the Agent.

【Example】

#Create a user user1, associated group group1, use md5 authentication method, authentication key is Hostname, no encryption.

Switch#configure terminal

Switch(config)#snmp-server user user1 group1 auth md5 auth-password Hostname

56.1.9 snmp-server user remote

【Command】

snmp-server user *user-name group-name* **remote** *ip-address* **[udp-port** *port-number* **]] [auth { md5 | sha }{ auth-password | auth-key }** *auth-value* **[priv des { priv-password | priv-key }** *priv-value* **]]**

no snmp-server user *user-name* **remote [** *ip-address* **[udp-port** *port-number* **]]**

【Config-mode】

Global Config-mode

【Parameter】

user-name: user name, in the form of a string, no longer than 32 characters.

group-name: the name of the group, in the form of a string, no longer than 32 characters.

ip-address: IP address, in dotted decimal form.

port-number: The udp port number, in the form of an integer, in the range of 1-65535.

auth: The security level is certified.

md5: Use MD5 hash function for authentication.

sha: Use SHA hash function for authentication.

auth-password *auth-value*: Authentication password, in string form, 8-32 characters long.

auth-key *auth-value*: MD5 authentication key, by combining with the hash function to generate the authentication code, so as to achieve the authentication function, MD5 authentication string length of 32 characters, SHA authentication string length of 40 characters.

priv-password *priv-value*: encrypted password, in string form, length 8-32 characters.

priv-key *priv-value*: The encryption key, which is combined with the hash function to generate the authentication code, is in the form of a string with a length of 32 characters.

【Description】

The **snmp-server user remote** command is used to configure the remote user information configuration for SNMPv3.

The **no snmp-server user user-name remote** command is used to remove the remote user configuration information for SNMPv3.

Notes

The security level of the user must be the same as the security level of the group. If the security level of the user is NoauthPriv, the security level of the group to which the user belongs must also be NoauthPriv, otherwise the user None effect, None method to access the Agent.

【Example】

#Create remote user user1, associate group1, use md5 authentication method, authentication key is Hostname, no encryption.

Switch#configure terminal

Switch(config)#snmp-server user user1 group1 remote 1.1.1.1 auth md5 auth-password Hostname

56.1.10 snmp-server enable { traps | informs }

【Command】

snmp-server enable {traps | informs } [bridge | gbn | gbnsavecfg | interfaces | rmon | snmp]*

no snmp-server enable traps/informs [bridge | gbn | gbnsavecfg | interfaces | rmon | snmp]*

【Config-mode】

Global Config-mode

【Parameter】

bridge: Indicates bridge-related announcements

gbn: Indicates gbn-related announcements

gbnsavecfg: Indicates that the configuration saves the associated announcements.

interfaces: Indicates interface-related announcements.

rmon: Indicates a notice from the rmon module.

snmp: Indicates the announcement of the snmp module.

【Description】

The **snmp-server enable {traps | informs}** command is used to enable the traps/informs function.

The **no snmp-server enable traps/informs** command is used to disable the traps/informs function.

If the traps function is enabled, the device will send traps information to the NMS when the device is running abnormally, such as interface down, so that users can know the device running status in time.

【Example】

#Enables the device to send Trap function to NMS.

Switch#configure terminal

Switch(config)#snmp-server enable traps

56.1.11 snmp-server host

【Command】

snmp-server host *ip-address* **[version { 1 | 2c | 3 }]** *security-name* **[udp-port** *port-number*] **[notify-type [bridge | gbn | gbnsavecfg | interfaces | rmon | snmp]*]**

no snmp-server host *ip-address security-name* **{ 1 | 2c | 3 }**

【Config-mode】

Global Config-mode

【Parameter】

ip-address: IP address in dotted decimal format: X.X.X.X.

1: Indicates SNMPv1 version.

2c: Indicates the SNMPv2 version, the default version.

3: Indicates SNMPv3 version.

security-name: The security name, in string form, is no more than 32 characters long; SNMP v1 and SNMP v2c use the community-name, and SNMP v3 uses the group name.

port-number: Port number, in the form of an integer, in the range of 1-65535, default value 162.

bridge: Indicates bridge-related announcements.

gbn: Indicates a gbn-related notice.

gbnsavecfg: Indicates a configuration-related announcement.

interfaces: Indicates interface-related announcements.

rmon: Indicates the announcement of the rmon function.

snmp: Indicates the announcement of the snmp function.

【Description】

The **snmp-server host** command is used to configure the destination address and other related parameters for sending a trap.

The **no snmp-server host** command is used to remove the send-trap destination address and other related parameters.

By default, no snmp-server host information is configured.

【Example】

#Create SNMPv2 Trap host with IP address 1.1.1.1 and security mode as group name test.

Switch#configure terminal

Switch(config)#snmp-server host 1.1.1.1 test

56.1.12 snmp-server trap-source

【Command】

snmp-server trap-source *ip-address*

no snmp-server trap-source

【Config-mode】

Global config-mode

【Parameter】

ip-address: IP address in dotted decimal format: X.X.X.X.

【Description】

The **snmp-server trap-source** command is used to configure the source address for sending trap messages.

The **no snmp-server trap-source** command is used to remove the source address configuration for sending trap messages.

【Example】

#Configure the source IP address of the trap message to be sent as 1.1.1.1.

Switch#configure terminal

Switch(config)#snmp-server trap-source 1.1.1.1

56.1.13 snmp-server engineid

【Command】

snmp-server engineid { local | remote *ip-address* **[udp-port** *port-number* **] }** *engine-id*

no snmp-server engineid { local | remote *ip-address* **[udp-port** *port-number* **] }**

【Config-mode】

Global config-mode

【Parameter】

local: Indicates that the local engine identifier is configured.

remote: Indicates that the remote engine identifier is configured.

ip-address: IP address in dotted decimal format: X.X.X.X.

port-number: UDP port number, integer form, value range 1-65535.

engine-id: Engine identifier, in string format, no more than 24 characters long.

【Description】

The **snmp-server engineid** command is used to configure the engine identifier.

The **no snmp-server engineid** command is used to remove the engine identification.

By default, there is a local engine identification configuration and no remote engine identification configuration.

【Example】

#Configure the engine ID of 192.168.1.10 at the remote end to be 12.

Switch#configure terminal

Switch(config)#snmp-server engineid remote 192.168.1.10 12

56.1.14 snmp-server max-packet-length

【Command】

snmp-server max-packet-length *length-value*

no snmp-server max-packet-length

【Config-mode】

Global config-mode

【Parameter】

length-value: The length of the message, integer form, value range 484-8000, in Byte.

【Description】

The **snmp-server max-packet-length** command is used to configure the maximum length of supported SNMP messages.

The **no snmp-server max-packet-length** command is used to remove the maximum length of supported SNMP messages.

By default, the supported maximum length is 1000 Bytes.

【Example】

#Configure the maximum supported SNMP length to 2000 Bytes.

Switch#configure terminal

Switch(config)#snmp-server max-packet-length 2000

56.2 SNMP Monitoring Command

56.2.1 show snmp-server community

【Command】

show snmp-server community

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

The **show snmp-server community** command is used to view the group information of SNMP.

【Example】

#View group information.

Switch(config)#show snmp-server community

Show snmp community information

index community priority state view-name

1 test rw permit iso

snmp-server community Display field descriptions

Field	Description
index	Index number
community	Group Name
priority	Access rights: ro, rw
state	Access control status: permit, deny
view-name	SNMP view name

56.2.2 show snmp-server contact

【Command】

show snmp-server contact

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

show **snmp-server contact** command is used to view the device manager's contact information.

【Example】

#View the contact information for the facility manager.

Switch(config)#show snmp-server contact

Manager contact information : http://

snmp-server contact Display field Description

Field	Description
Manager contact information	Contact Information

56.2.3 show snmp-server engineid

【Command】

show snmp-server engineid { local | remote }

【Config-mode】

Arbitrary Config-mode

【Parameter】

local: Local engine ID.

remote: Remote engine ID.

【Description】

show **snmp-server engineid** command is used to display the information of the proxy engine ID.

【Example】

#View the engine ID information of this end.

Switch(config)#show snmp-server engineid local

The information about local engine is followed:

Local engine id:543670000000000000000000

snmp-server engined display fields description

Field	Description

Local engine id	Local SNMP engine ID

56.2.4 show snmp-server group

【Command】

show snmp-server group

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

The **show snmp-server group** command is used to display information about SNMP agent groups.

【Example】

#View SNMP agent group information.

Switch(config)#show snmp-server group

groupname: initial

securitymodel: 3 noauthpriv

readview: iso

writeview: iso

notifyview: iso

context: default value(NULL)

groupname: initial

securitymodel: 3 auth

readview: iso

writeview: iso

notifyview: iso

context: default value(NULL)

snmp-server group Display field description

Field	Description
groupname	SNMP agent group name
securitymodel	Security model: noauthpriv, auth, priv
readview	Read view name
writeview	Write view name
notifyview	Notice view name
context	Contextual environments

56.2.5 show snmp-server host

【Command】

show snmp-server host

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

The **show snmp-server** host command is used to display information about SNMP agent trap hosts.

【Example】

#View SNMP target host information.

Switch(config)#show snmp-server host

Show SNMP trap host information

SNMP host ip security version

1.1.1.1 test 1

snmp-server host Display fields description

Field	Description
SNMP host ip	The IP address of the target host receiving the Trap
security	Security Name
version	SNMP version: 1, 2c, 3

56.2.6 show snmp-server location

【Command】

show snmp-server location

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

show **snmp-server location** command is used to display device location information.

【Example】

#View device location information.

Switch(config)#show snmp-server location

Switch location information : sample sysLocation factory default

snmp-server location Display field description

Field	Description
Switch location information	Geolocation information of the device

56.2.7 show snmp-server max-packet-length

【Command】

show snmp-server max-packet-length

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

The **show snmp-server max-packet-length** command is used to display the supported maximum SNMP message length.

【Example】

#View the statistics of SNMP.

Switch(config)#show snmp-server max-packet-length

snmp max-packet-length: 1000 Bytes.

snmp-server location Display field description

Field	Description
snmp max-packet-length	Maximum length of SNMP messages

56.2.8 show snmp-server name

【Command】

show snmp-server name

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

The **show snmp-server name** command is used to display SNMP agent system name information.

【Example】

#View SNMP agent system name information.

Switch(config)#show snmp-server name

system name : system-name

snmp-server name Display field description

Field	Description
system name	System name, the value is determined by the system model

56.2.9 show snmp-server notify

【Command】

show snmp-server notify

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

The **show snmp-server notify** command is used to display SNMP agent notification configuration information.

【Example】

#View SNMP agent announcement configuration information.

Switch(config)#show snmp-server notify

Name Type State

bridge trap disabled

gbn trap disabled

gbnsavecfg trap disabled

interfaces trap disabled

rmon trap disabled

snmp trap disabled

snmp-server notify display field description

Field	Description
Name	Notice Type

Type	Message Type: trap、inform
State	Notification enable status: enabled、disabled

56.2.10 show snmp-server user

【Command】

show snmp-server user

【Config-mode】

Arbitrary Config-mode

【Parameter】

None

【Description】

The **show snmp-server user** command is used to display the user information of the SNMP agent.

【Example】

#View the user information of the SNMP agent.

Switch(config)#show snmp-server user

User name: initialmd5

Engine ID: 54367000000000000000000

Authentication Protocol: HMACMD5AuthProtocol

Group-name: initial

Validation: valid

User name: initialsha

Engine ID: 54367000000000000000000

Authentication Protocol: HMACSHAAuthProtocol

Group-name: initial

Validation: valid

User name: initialnone

Engine ID: 543670000000000000000000

Authentication Protocol: NoauthProtocol

Group-name: initial

Validation: valid

snmp-server user display field description

Field	Description
User name	User Name
Engine ID	SNMP Engine ID
Authentication Protocol	Certification Agreement: NoauthProtocol、AuthProtocol
Group-name	The name of the referenced SNMP group
Validation	Validity: valid、invalid

56.2.11 show snmp-server view

【Command】

show snmp-server view

【Config-mode】

Global config-mode

【Parameter】

None

【Description】

The **show snmp-server view** command is used to display SNMP view information.

【Example】

#View the SNMP view information.

Switch(config)#show snmp-server view

View Name Subtree Type

iso 1 Include

sysview 1.3.6.1.2.1.1Include

Internet1.3.6.1Include

snmp-server user display field description

Field	Description
View Name	View Name
Subtree	The OID of the subtree corresponding to the view
Type	Type: included、exclude

56.2.12 debug snmp

【Command】

debug snmp

no debug snmp

【Config-mode】

Global config-mode

【Parameter】

None

【Description】

The **debug snmp** command is used to turn on the debugging function of the SNMP module.

The **no debug snmp** command is used to turn off the debugging function of the SNMP module

【Example】

#Turn on the debugging function of SNMP module.

Switch#configure terminal

Switch(config)#debug snmp

Chapter 57 RMON

57.1 RMON Configuration Command

57.1.1 rmon event

【Command】

rmon event *event-id* **[description** *description-value* **] { none | log | trap** *community-value* **| log-trap** *community-value* **}** **[owner** *owner-value* **]**

no rmon event [*event-id* **]**

【Config-mode】

Global config-mode

【Parameter】

event-id: The event group sequence number, with a value range of 1-65535.

description-value: Description information, up to 127 strings.

community-value: The name of the group, up to 127 strings.

owner-value: Name, up to 127 characters.

log: Indicates that an alarm log message is generated when an event is triggered.

trap: Indicates that an SNMP trap notification is sent when an event is triggered.

log-trap: Indicates that when an event is triggered, both the alarm log and the SNMP trap notification sent are generated.

none: Indicates that no processing is done when the event is triggered.

【Description】

The **rmon event** command is used to configure the event group.

The **no rmon event** command is used to remove the event group configuration.

By default, no event group information is configured.

SNMP-related functions need to be configured when the processing mode is trap or log-trap.

【Example】

#Configure event group 1, processing as log.

Switch#configure terminal

Switch(config)#rmon event 1 log

57.1.2 rmon alarm

【Command】

rmon alarm *alarm-id oid-value interval-value* **{ absolute | delta } rising** *rising-value rising-event-id* **falling** *falling-value falling-event-id* **[owner** *owner-value* **]**

no rmon alarm [*index-id* **]**

【Config-mode】

Global config-mode

【Parameter】

alarm-id: Alarm group sequence number, the value range is 1-65535.

oid-value: Configure the object instances that need to be remotely monitored.

interval-value: Sampling interval, the value range is 2-3600, in seconds.

absolute: Indicates that the configuration alarm group sampling type is absolute.

absolute: Indicates that the configuration alarm group sampling type is a relative value.

rising-value: Configure the rising threshold value, which takes values from 1 to 2147483647.

rising-event-id: The sequence number of the event that is triggered to the rising threshold value to occur, taking values from 1-65535.

falling-value: Configure the threshold value for the drop, which takes the value range of 1 to 2147483647.

falling-event-id: The sequence number of the event that is triggered to the falling threshold value to occur, takes a value in the range of 1-65535.

owner-value: Name, up to 127 characters.

【Description】

The **rmon alarm** command is used to set the alarm group and configure the alarm trigger conditions.

The **no rmon alarm** command is used to delete the alarm group configuration.

By default, no alarm group information is configured.

The alarm group rise/fall threshold ID should be the same as the event group sequence number, otherwise no event action will be generated.

【Example】

#Configure monitoring OID 1.3.6.1.2.1.2.2.1.10.1, sampling interval is 5s, sampling type uses absolute value, rising value over 3000 will alarm and trigger event 1, falling value over 2000 will alarm and trigger event 1.

Switch#configure terminal

Switch(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.10.1 5 absolute rising 3000 1 falling 2000 1

57.1.3 rmon statistics

【Command】

rmon statistics *statistics-id* **[owner** *owner-value* **]**

no rmon statistics [*index-id* **]**

【Config-mode】

Port Config-mode

【Parameter】

statistics-id: Statistical group sequence number, the value range is 1-65535.

owner-value: Name, up to 127 characters.

【Description】

The **rmon statistics** command is used to configure statistics group information.

The **no rmon statistics** command is used to remove the configuration.

By default, no statistics group information is configured.

【Example】

#Configure statistics group 1 in port 0/0/1 mode.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#rmon statistics 1

57.1.4 rmon history

【Command】

rmon history *history-id* **bucket** *bucket-value* **interval** *interval-value* **[owner** *owner-value* **]**

no rmon history [*index-id* **]**

【Config-mode】

Port Config-mode

【Parameter】

index-id: History group sequence number with a value range of 1-65535.

bucket-value: The number of sampled records, with values ranging from 1 to 65535.

interval-value: Sampling interval, the value range is 1-3600, in seconds.

owner-value: Name, up to 127 characters.

【Description】

The **rmon history** command is used to configure history group statistics.

The **no snmp-server location** command is used to remove the history group configuration.

By default, no history group information is configured.

【Example】

#Configure history group 1 in port 0/0/1 mode with a sampling number of 1 and a sampling interval of 10s.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#rmon history 1 buckets 1 interval 10

57.2 RMON Monitoring Command

57.2.1 show rmon alarm

【Command】

show rmon alarm [*alarm-id* **]**

【Config-mode】

Arbitrary Config-mode

【Parameter】

alarm-id: Alarm group sequence number, the value range is 1-65535.

【Description】

The **show rmon alarm** command is used to display the configured RMON alarm information.

【Example】

#View the alarm information configured by the device.

Switch(config)#show rmon alarm

AlarmEntry 1:

Variable : 1.3.6.1.2.1.2.2.1.10.1

Interval: 5

Type : absolute

Rising : threshold 3000 event index 1

Falling : threshold 2000 event index 1

Last value : 1

Owner : NULL

rmon alarm display field description

Field	Description

AlarmEntry 1	Alarm group serial number
Variable	Monitoring object: OID
Interval	Sampling time interval
Type	Sampling Type
Rising	Upward threshold value
Falling	Lowering the threshold value
Last value	Last value
Owner	Affiliated user name

57.2.2 show rmon event

【Command】

show rmon event [*event-id*]

【Config-mode】

Arbitrary Config-mode

【Parameter】

event-id: The event group sequence number, with a value range of 1-65535.

【Description】

The **show rmon event** command is used to display the configured RMON event information.

【Example】

#View the RMON event information of the device.

Switch(config)#show rmon event

EventEntry 1:

Description : NULL

Type : log

Community : NULL

Owner : NULL

show rmon event Display field description

Field	Description
EventEntry 1	Event Group Serial Number
Description	Event description information
Type	Event Type
Community	SNMP group name
Owner	Affiliated user name

57.2.3 show rmon eventlog

【Command】

show rmon eventlog *event-id*

【Config-mode】

Arbitrary Config-mode

【Parameter】

event-id: The event group sequence number, with a value range of 1-65535.

【Description】

The show rmon eventlog command is used to view event log information.

【Example】

#View event log information

Switch(config)#show rmon eventlog

57.2.4 show rmon history

【Command】

show rmon history interface [ethernet *port-id* **]***

【Config-mode】

Arbitrary Config-mode

【Parameter】

port-id: Port number, the configuration range is determined by the switch hardware model.

【Description】

The **show rmon history** command is used to display history group information.

【Example】

#View the history group information of port 0/0/1.

Switch(config)#show rmon history interface ethernet 0/0/1

HistoryControlEntry 1:

Interface : e0/0/1

Owner : NULL

Interval : 10

Buckets : 1

History record 1: 0 days 0 hours 8 minutes 38 seconds

DropEvents : 0, Octets : 0, Pkts : 0

BroadcastPkts : 0, MulticastPkts: 0, CRCAlignErrors: 0

UndersizePkts : 0, OversizePkts : 0, Fragments : 0

Jabbers : 0, Collisions : 0, Utilization : 0

show rmon history Display field description

Field	Description
HistoryControlEntry 1	History Group Serial Number
Interface	Port number
Owner	History Group Owners
Interval	Sampling interval
Buckets	Number of time interval samples
History record 1	History Group Record Number
DropEvents	Number of message drops
Octets	Statistics of bytes received
Pkts	Statistics on the number of messages received
BroadcastPkts	Number of broadcast messages received
MulticastPkts	Number of multicast messages received
CRCAlignErrors	Number of messages received with lengths between 64 bytes and 1518 bytes and with FCS checksum errors or sequence number errors.

UndersizePkts	Number of messages received with length less than 64 bytes.
OversizePkts	Number of messages received with length greater than 1518 bytes.
Fragments	Number of messages received with length less than 64 bytes and with FCS checksum or sequence number errors
Jabbers	Number of messages received that are greater than 1518 bytes in length and have both FCS check errors or sequence errors
Collisions	Number of conflicting messages
Utilization	Utilization rate

57.2.5 show rmon statistics

【Command】

show rmon statistics [ethernet *port-id* **] ***

【Config-mode】

Arbitrary Config-mode

【Parameter】

port-id: Port number, the configuration range is determined by the switch hardware model.

【Description】

The show rmon statistics command is used to display statistics group information.

【Example】

#View port 0/0/1 statistics group information.

Switch(config)#show rmon statistics

EtherStatsEntry 1:

Interface : e0/0/1

Owner : NULL

Octets : 0, Pkts : 0, BroadcastPkts : 0

MulticastPkts : 0, CRCAlignErrors : 0, UndersizePkts : 0

OversizePkts : 0, Fragments : 0, Jabbers : 0

Collisions : 0, DropEvents : 0, Pkts64 : 0

Pkts65to127 : 0, Pkts128to255 : 0, Pkts256to511 : 0

Pkts512to1023 : 0, Pkts1024to1518 : 0

show rmon statistics Display field description

Field	Description
EtherStatsEntry 1	Statistical group serial number
Interface	Port number
Owner	Statistical Group Owners
Octets	Statistics of bytes received
Pkts	Statistics on the number of messages received
BroadcastPkts	Number of broadcast messages received
MulticastPkts	Number of multicast messages received
CRCAlignErrors	Number of messages received with lengths between 64 bytes and 1518 bytes and with FCS checksum errors or sequence number errors
UndersizePkts	Number of messages received with length less than 64 bytes

OversizePkts	Number of messages received with length greater than 1518 bytes
Fragments	Number of messages received with length less than 64 bytes and with FCS checksum or sequence number errors
Jabbers	Number of messages received that are greater than 1518 bytes in length and also have an FCS check error or sequence error
Collisions	Number of conflicting messages
DropEvents	Number of message drops
Pkts64	Number of 64-byte messages received
Pkts65to127	Number of messages received between 65 bytes and 127 bytes
Pkts128to255	Number of messages received between 128 bytes and 255 bytes
Pkts256to511	Number of messages received between 256 bytes and 511 bytes
Pkts512to1023	Number of messages received between 512 bytes and 1023 bytes
Pkts1024to1518	Number of messages received between 1024 bytes and 1518 bytes

57.2.6 debug rmon

【Command】

debug rmon

no debug rmon

【Config-mode】

Global config-mode

【Parameter】

None

【Description】

The **debug rmon** command is used to turn on the debugging function of the rmon module.

The **no debug rmon** command is used to turn off the debugging function of the rmon module.

【Example】

#Turn on the debugging function of the rmon module.

Switch#configure terminal

Switch(config)#debug rmon

Chapter 58 Port Mirror

58.1 Port mirror configuration commands

58.1.1 mirror group id source-interface

【Command】

mirror group *group-id* **source-interface {{ ethernet** *port-id* **}* | cpu} { ingress| egress | both }**

no mirror group *group-id* **source-interface {{ ethernet** *port-id* **}* | cpu }**

【Config-mode】

Global Config-mode

【Parameters】

group-id: group number, the value range is 1-3.

port-id: port number, the configuration range is determined by the switch hardware model.

cpu: indicates the mirroring cpu port.

ingress: indicates the message in the mirroring input direction.

egress: indicates mirroring of messages in the output direction.

both: means mirroring the messages in the input and output directions at the same time.

【Description】

The **mirror group group-id source-interface** command is used to configure the mirror source port.

The **mirror group group-id source-interface** command is used to delete the mirror source port configuration.

After the mirroring function takes effect, the messages in the specified direction of the mirror source are copied to the monitoring port.

Notes:

Multiple mirroring source ports are allowed, but only one mirroring destination port is allowed, and the mirroring source port and destination port cannot be the same port.

【Example】

#Configure mirroring group 1 source port as 0/0/1 and mirror the messages in the input direction.

Switch#configure terminal

Switch(config)#mirror group 1 source-interface ethernet 0/0/1 ingress

58.1.2 mirror group id destination-interface

【Command】

mirror group *group-id* **destination-interface ethernet** *port-id*

no mirror group *group-id* **destination-interface ethernet** *port-id*

【Config-mode】

Global Config-mode

【Parameter】

group-id: The group number, range 1-3.

port-id: Port number, the configuration range is determined by the switch hardware model.

【Description】

The **mirror group** *group-id* **destination-interface ethernet** command is used to configure the mirror destination port.

The **mirror group** *group-id* **destination-interface ethernet** *port-id* command is used to remove the mirror destination port.

The messages of the mirror source port are copied to the mirror destination port according to the configured mirroring rules to facilitate monitoring of the network operation.

【Example】

#Configure port 0/0/1 as the mirroring destination port for mirroring group 1.

Switch#configure terminal

Switch(config)#mirror group 1 destination-interface ethernet 0/0/1

58.1.3 no mirror group all

【Command】

no mirror group all

【Config-mode】

Global Config-mode

【Parameters】

None

【Description】

The **no mirror group all** command is used to configure all mirror configurations.

【Example】

#Delete all mirror configurations.

Switch#configure terminal

Switch(config)#no mirror group all

58.2 Remote mirroring configuration commands

58.2.1 mirror group id source-interface

【Command】

mirror group *group-id* **source-interface {{ ethernet** *port-id* **}* | cpu} { ingress| egress | both }**

no mirror group *group-id* **source-interface {{ ethernet** *port-id* **}* | cpu }**

【Config-mode】

Global Config-mode

【Parameter】

group-id: group number, the value range is 1-3.

port-id: port number, the configuration range is determined by the switch hardware model.

cpu: indicates the cpu port.

ingress: indicates the message in the mirroring input direction.

egress: indicates the mirroring of messages in the output direction.

both: indicates the simultaneous mirroring of messages in the input and output directions.

【Description】

The **mirror group** *group-id* **source-interface** command is used to configure the mirror source port.

The **mirror group** *group-id* **source-interface** command is used to delete the mirror source port configuration.

After the mirroring function takes effect, the messages in the specified direction of the mirror source are copied to the monitoring port.

Notes:

Multiple mirroring source ports are allowed, but only one mirroring destination port is allowed, and the mirroring source port and destination port cannot be the same port.

【Example】

#Configure mirroring group 1, with source port 0/0/1, to mirror messages in the input direction.

Switch#configure terminal

Switch(config)#mirror group 1 source-interface ethernet 0/0/1 ingress

58.2.2 mirror group id destination-interface ethernet port-id rspan local

【Command】

mirror group *group-id* **destination-interface ethernet** *port-id* **rspan local vid** *vlan-id*

【Config-mode】

Global Config-mode

【Parameter】

group-id: the group number, range 1-3.

port-id: port number, the configuration range is determined by the switch hardware model.

local: indicates that this device is the starting device for remote mirroring streams.

vlan-id: vlan id, the range of values is 1-4094.

【Description】

The **mirror group** *group-id* **destination-interface ethernet** *port-id* **rspan local** command is used to configure the monitoring port of the remote mirroring origin device and specify the vlan for mirror stream encapsulation.

The **no mirror group** *group-id* **destination-interface ethernet** *port-id* **rspan local** command is used to remove the local configuration of remote mirroring.

The messages from the mirror source port are copied to the monitor port according to the mirroring rules and encapsulated with the specified vlan.

The remote mirroring VLAN must be created and the monitor port must be added as a member, and the monitor port must be configured as trunk.

When a VLAN is designated as a remote mirroring VLAN, it is recommended that the VLAN not be used for other purposes.

All devices through which the remote mirroring flow passes must use the same remote mirroring VLAN, and the mac table entries of the corresponding VLAN will not be learned on the middle and target devices.

The same port can only be one of the roles in rspan { local | middle | target }.

【Example】

#Configure remote mirroring group 1 with monitoring port 0/0/2, device role local, and encapsulation vlan 100.

Switch#configure terminal

Switch(config)#mirror group 1 destination-interface ethernet 0/0/2 rspan local vid 100

58.2.3 mirror group id destination-interface ethernet port-id rspan middle

【Command】

mirror group *group-id* **destination-interface ethernet** *port-id* **rspan middle vid** *vlan-id*

no mirror group *group-id* **destination-interface ethernet** *port-id* **rspan middle vid** *vlan-id*

【Config-mode】

Global Config-mode

【Parameters】

group-id: group number, the value range is 1-3.

port-id: port number, the configuration range is determined by the switch hardware model.

middle: Indicates that this device is the middle device through which the remote mirror stream passes.

vlan-id: vlan id, the value range is 1-4094.

【Description】

The **mirror group** *group-id* **destination-interface ethernet** *port-id* rspan middle command is used to configure the monitoring port of the remote mirroring intermediate device and specify the vlan for mirroring stream encapsulation.

The no mirror group group-id destination-interface ethernet port-id rspan middle command is used to remove the remote mirroring intermediate device configuration.

The remote mirror vlan must be created and contain two members: the port connected to the monitor port on the rspan local device and the monitor port of the rspan middle device, and ensure that the encapsulated vlan is tagged with forwarding.

The same port can only be one of the roles in rspan { local | middle | target }.

【Example】

#Configure remote mirroring group 1, port 0/0/2 as the monitor port, and the device role as middle, encapsulation vlan 100.

Switch#configure terminal

Switch(config)#mirror group 1 destination-interface ethernet 0/0/2 rspan middle vid 100

58.2.4 mirror group id destination-interface ethernet port-id rspan target

【Command】

mirror group *group-id* **destination-interface ethernet** *port-id* **rspan target vid** *vlan-id*

no mirror group *group-id* **destination-interface ethernet** *port-id* **rspan target vid** *vlan-id*

【Config-mode】

Global Config-mode

【Parameters】

group-id: The group number,range 1-3.

port-id: Port number, the configuration range is determined by the switch hardware model.

target: Indicates that this device is a terminal device for remote mirroring streams.

vlan-id: vlan id, range 1-4094.

【Description】

The **mirror group** *group-id* **destination-interface ethernet** *port-id* **rspan target** command is used to configure the monitoring port of the remote mirror terminal device and specify the vlan for mirroring stream encapsulation.

The **no mirror group** *group-id* **destination-interface ethernet** *port-id* **rspan target** command removes the configuration of the remote mirror terminal device.

The remote mirror vlan must be created and contain two members: the port connected to the monitor port of the rspan middle device, and the monitor port of the rspan target device.

The same port can only be one of the roles in rspan { local | middle | target }.

【Example】

#Configure remote mirroring group 1, port 0/0/2 as the monitor port, device role as target, and encapsulation vlan 100.

Switch#configure terminal

Switch(config)#mirror group 1 destination-interface ethernet 0/0/2 rspan target vid 100

58.2.5 no mirror group all

【Command】

no mirror group all

【Config-mode】

Global Config-mode

【Parameter】

None

【Description】

The **no mirror group all** command is used to configure all mirror configurations.

【Example】

#Delete all mirror configurations.

Switch#configure terminal

Switch(config)#no mirror group all

58.3 Mirror monitor commands

58.3.1 show mirror group

【Command】

show mirror group { **all** | *group-id* }

【Config-mode】

Arbitrary Config-mode

【Parameters】

group-id: The group number, taking values in the range of 1-3.

【Description】

The **show mirror group** command is used to display mirroring configuration information.

【Example】

#View the configuration information of Set Mirror Group 1.

Switch(config)#show mirror group 1

Information about mirror groups:

Group number : 1

The monitor port : None

The mirrored egress ports :

The mirrored ingress ports :

Total entries: 1 .

show mirror group display field descriptions

Field	Description
Group number	Group number
The monitor port	Monitor port
The mirrored egress ports	Mirror the port number of incoming packets
The mirrored ingress ports	Mirror the port number of the input direction message

58.3.2 debug mirror

【Command】

debug mirror

no debug mirror

【Config-mode】

Global Config-mode

【Parameters】

None

【Description】

The **debug mirror** command is used to turn on the debugging function of the mirror module.

The **no debug mirror** command is used to turn off the debugging function of the mirror module.

【Example】

#Turn on the debugging function of the mirror module.

Switch#configure terminal

Switch(config)#debug mirror

Chapter 59 LLDP

59.1 LLDP Configure Cmomands

59.1.1 lldp

【command】

lldp

no lldp

【config-mode】

Global/port config-mode

【parameter】

None

【description】

lldp command is used to enable lldp.

no lldp command is used to disable lldp.

By default,lldp is disabled in global mode,and the port enabls lldp.

【example】

Enable lldp function globally.

Switch#configure terminal

Switch(config)#lldp

59.1.2 lldp hello-time

【command】

lldp hello-time *time-value*

no lldp hello-time

【config-mode】

Global config-mode

【parameter】

time-value: Time period, integer, range 5-32768, in seconds.

【description】

lldp hello-time *time-value* command is used to set the interval for sending LLDP packets to neighbors.

no lldp hello-time command is used to restore the default interval for the device to send LLDP packets to the neighbor device.

By default, the interval for sending LLDP packets is 30 seconds.

【example】

Set the LLDP sending interval to 10 seconds.

Switch#configure terminal

Switch(config)#lldp hello-time 10

59.1.3 lldp hold-time

【command】

lldp hold-time *time-value*

no lldp hold-time

【config-mode】

Global config-mode

【parameter】

time-value: multiple of time, integer, range 2-10, The default value is 4.

【description】

lldp hold-time *time-value* command is used to configure multiple of hold time. The default value is 4.

no lldp hold-time command is used to delete the multiple of hold time.

【example】

#Set multiple of hold time to 3.

Switch#configure terminal

Switch(config)#lldp hold-time 3

59.1.4 lldp trap

【command】

lldp trap { enable | disable }

【config-mode】

Global config-mode

【parameter】

None

【description】

lldp trap enable command is used to enable lldp trap.

lldp trap disable command is used to disable lldp trap.

By default,lldp trap is disabled.

lldp trap needs to be used with SNMP.

【example】

Enable lldp trap.

Switch#configure terminal

Switch(config)#lldp trap enable

59.1.5 lldp { rx | tx | rxtx }

【command】

lldp {rx | tx | rxtx }

no lldp

【config-mode】

Port config-mode

【parameter】

rx: Only receive lldp packets.

tx: Only send lldp packet.

rx: Both receive and send lldp packets.

【description】

lldp { rx | tx | rxtx } command is used to set how the port works.

no lldp command is used to disable lldp.

By default, port works at **rxtx**.

【example】

Configure port 0/0/1 to receive lldp packets only.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#lldp rx

59.1.6 lldp management-address

【command】

lldp management-address { vlan-interface | supervlan-interface } *if-id*

no lldp management-address

【config-mode】

Port config-mode

【parameter】

if-id: vlan interface id, integer form, normal vlan interface id range is 1-4094, supervlan interface id rang is 1-128.

【description】

lldp management-address { vlan-interface | supervlan-interface } command is used to set the lldp management address.

no lldp management-address command is used to delete the management address.

By default,there is no management address.

【example】

#Set interface vlan 1 as the lldp management address interface.

Switch#configure terminal

Switch(config)#interface ethernet 0/0/1

Switch(config-if-ethernet-0/0/1)#lldp management-address vlan-interface 1

59.2 LLDP Debug Commands

59.2.1 show lldp

【command】

show lldp [ethernet *port-id* **[to ehternet** *port-id***] *]**

【config-mode】

Any config-mode

【parameter】

port-id: Port number. string format: device number/slot number/port number,such as 0/0/1 .

【description】

show lldp command is used to display the lldp configuration and neighbor information.

【example】

#Display the lldp information of interface ethernet 0/0/2.

Switch(config)#show lldp ethernet 0/0/2

System LLDP: enable

LLDP trap: disable

LLDP hello-time: 30(s) LLDP hold-time: 4 LLDP TTL: 120(s)

Interface Ethernet 0/0/2

Port LLDP: rxtx Pkt Tx: 5 Pkt Rx: 3

Total neighbor count: 1

Neighbor (1):

TTL: 100(s)

Chassis ID: 28:3b:82:00:03:ee

Port ID: eth17

System Name: SWITCH

System Description: Switch

Port Description: NULL

Port Vlan ID: 1

Port SetSpeed: auto

Port ActualSpeed: FULL-1000

Port Link Aggregation: support ,not in aggregation

59.2.2 debug lldp

【command】

debug lldp

no debug lldp

【config-mode】

Global config-mode

【parameter】

None

【description】

debug lldp command is used to enable the lldp debugging.

no debug lldp command is used to disable the lldp debugging.

【example】

Enable the lldp debugging.

Switch#configure terminal

Switch(config)#debug lldp