S5300-12S Switch CLI Reference Guide

Models: S5300-12S

CLI Reference Guide

Contents

Chapter 1 802.1x Configuration Commands 1

1.1 dot1x enable 1
1.2 dot1x port-control 1
1.3 dot1x authentication multiple-hosts 2
1.4 dot1x authentication multiple-auth 3
1.5 dot1x default 3
1.6 dot1x reauth-max 4
1.7 dot1x re-authentication 4
1.8 dot1x timeout quiet-period 5
1.9 dot1x timeout re-authperiod 6
1.9.1 dot1x timeout tx-period 6
1.10 dot1x mab 7
1.11 dot1x mabformat 8
1.12 dot1x user-permit 8
1.12.1 dot1x user-permit 8
1.13 1dot1x authentication method 9
1.14 dot1x accounting enable 10
1.15 dot1x accounting method 11
1.16 dot1x authen-type, dot1x authentication type 11
1.17 dot1x guest-vlan 12
1.18 dot1x guest-vlan id 13
1.18.1 dot1x guest-vlan id 13
1.19 dot1x forbid multi-network-adapter 14
1.20 dot1x keepalive 14
1.21 aaa authentication dot1x 15
1.22 debug dot1x errors 15
1.23 debug dot1x state 16
1.24 debug dot1x packet 16
1.25 show dot1x 17

Chapter 2 Anti-Attack Configuration Commands 19

2.1 Anti-AttaAnti-Attack Configuration Commands 19
2.1.1 filter period 19
2.1.2 filter threshold 19
2.1.3 filter block-time 20
2.1.4 filter polling period 21
2.1.5 filter polling threshold 21
2.1.6 filter polling auto-fit 22
2.1.7 filter igmp 23
2.1.8 filter ip source-ip 23
2.1.9 filter icmp 24
2.1.10 filter icmpv6 24
2.1.11 filter dhcp 25
2.1.12 filter arp 25
2.1.13 filter bpdu 26
2.1.14 filter mode 26
2.1.15 filter enable 27
2.1.16 filter shutdown-action 27

2.1.17 show filter 28

Chapter 3 Backup Link Configuration Commands 30

3.1 Global Configuration Commands 30
3.1.1 backup-link-group *id* 30
3.1.2 backup-link-group id preemption-mode forced {delay *value*} 30
3.1.3 backup-link-group id preemption-mode bandwidth {delay *value*} 31
3.1.4 monitor-link-group id 32
3.2 Port Configuration Commands 33
3.2.1 backup-link-group id active 33
3.2.2 backup-link-group id backup 34
3.2.3 share-load vlan vlanmap 34
3.2.4 backup-link-group mmu transmit 35
3.2.5 backup-link-group mmu receive 36
3.2.6 monitor-link-group id uplink 37
3.2.7 monitor-link-group id downlink 37
3.3 how Configuration Commands 38
3.3.1 show backup-link-group id 38
3.3.2 show monitor-link-group id 39

Chapter 4 System Management Commands 41

4.1 File Management Configuration Commands 41
4.1.1 copy 41
4.1.2 delete 42
4.1.3 dir 42
4.1.4 ip address 43
4.1.5 ip route 43
4.1.6 show configuration 44
4.1.7 format 44
4.1.8 more 45
4.2 Basic System Management Commands 46
4.2.1 boot flash 46
4.2.2 cd 46
4.2.3 chinese 47
4.2.4 date 47
4.2.5 english 48
4.2.6 md 48
4.2.7 pwd 49
4.2.8 rd 49
4.2.9 rename 50
4.2.10 reboot 51
4.2.11 alias 51
4.2.12 boot system flash 52
4.2.13 help 52
4.2.14 history 53
4.2.15 show 54
4.2.16 show alias 55
4.2.17 show break 56

Chapter 5 Terminal Service Configuration Commands 57

5.1 Telnet Configuration Commands 57
5.1.1 telnet 57

5.1.2 ip telnet 58
5.1.3 ctrl-shift-6+x (the current connection is mounted) 60
5.1.4 where 60
5.1.5 resume 61
5.1.6 disconnect 62
5.1.7 clear telnet 64
5.1.8 show telnet 64
5.1.9 debug telnet 65
5.2 Terminal Configuration Commands 65
5.2.1 attach-port 65
5.2.2 autocommand 66
5.2.3 clear line 67
5.2.4 connect 67
5.2.5 disconnect 67
5.2.6 exec-timeout 68
5.2.7 length 68
5.2.8 line 69
5.2.9 location 69
5.2.10 login authentication 70
5.2.11 monitor 70
5.2.12 no debug all 71
5.2.13 password 71
5.2.14 resume 72
5.2.15 show debug 72
5.2.16 show line 73
5.2.17 terminal length 73
5.2.18 terminal monitor 74
5.2.19 terminal width 74
5.2.20 terminal-type 75
5.2.21 where 76
5.2.22 width 76

Chapter 6 Maintenance and Debugging Tool Commands 77

6.1 Network Testing Tool Commands 77
6.1.1 ping 77
6.1.2 traceroute 79
6.2 Fault Diagnosis Commands 81
6.2.1 logging 81
6.2.2 logging buffered 82
6.2.3 logging console 83
6.2.4 logging facility 84
6.2.5 logging monitor 85
6.2.6 logging on 87
6.2.7 logging trap 88
6.2.8 logging command 89
6.2.9 logging source-interface 90
6.2.10 logging history alerts 90
6.2.11 logging history critical 90
6.2.12 logging history debugging 91
6.2.13 logging history emergencies 91
6.2.14 logging history errors 92
6.2.15 logging history informational 92

6.2.16 logging history notifications 93
6.2.17 logging history warnings 93
6.2.18 logging history rate-limit 93
6.2.19 logging history size 94
6.2.20 service timestamps 94
6.2.21 clear logging 95
6.2.22 show break 96
6.2.23 show debug 97
6.2.24 show logging 98

Chapter 7 SSH Configuration Commands 100

7.1 ip sshd enable 100
7.2 ip sshd timeout 100
7.3 ip sshd auth-method 101
7.4 ip sshd access-class 101
7.5 ip sshd auth-retries 102
7.6 ip sshd clear 103
7.7 ip sshd silence-period 103
7.8 ip sshd version 2 104
7.9 ip sshd Ciphers 105
7.9.1 ip sshd KexAlgorithms 105
7.10 ip sshd MACs 106
7.11 ip sshd sftp 106
7.12 ip sshd save 107
7.13 ssh 107
7.14 show ssh 108
7.15 show ip sshd 109

Chapter 8 Virtualization Configuration Commands 110

8.1 bvss 110
8.2 bvss enable 110
8.3 bvss domain-id 111
8.4 bvss member-id 111
8.5 bvss mode 112
8.6 bvss priority 112
8.7 bvss interface 113
8.8 bvss mac-address mode 114
8.9 show bvss 114
8.10 debug bvss 116
8.11 Configuration Example 117

Chapter 9 CFM Configuration Commands Overview 118

9.1 Stipulation 118
9.1.1 Format Stipulation in the Command Line 118

Chapter 10 CFM 119

10.1 CFM Configuration Commands 119
10.1.1 Adding the Maintenance Domain and Entering the Maintenance Domain Mode 119
10.1.2 Deleting the Maintenance Domain 119
10.1.3 Browsing the Maintenance Domain 120
10.1.4 Adding a Maintenance Association 120
10.1.5 Deleting the Maintenance Association 121

10.1.6 Browsing the Maintenance Association 122
10.1.7 Adding MIP 123
10.1.8 Deleting MIP 123
10.1.9 Browsing MIP 124
10.1.10 Adding MEP 125
10.1.11 Deleting MEP 126
10.1.12 Browsing MEP 126
10.2 CFM Maintenance Commands 128
10.2.1 Loopback 128
10.2.2 Linktrace 128
10.2.3 Deleting the Linktrace Result Table 129
10.2.4 Setting the Size of the Linktrace Result Table 130
10.2.5 Setting the Number of Entries in the Linktrace Result Table 130
10.2.6 Setting the Aging Time of the Linktrace Result Table 131
10.2.7 Deleting the MEP Statistics Data 132
10.3 CFM Control Commands 132
10.3.1 CFM Stack Control Command 132
10.3.2 CFM Interface Control Command 133
10.3.3 MIP Control Command 133
10.4 CFM Query Commands 133
10.4.1 Browsing the CFM Protocol Stack 133
10.4.2 Browsing the CFM Interface 134
10.4.3 Browsing the Locally Stored Information about the Remote MEP 134
10.4.4 Browsing the LinkTrace Result Table 135
10.4.5 Browsing the Whole Running Status of CFM 137
10.5 Y.1731 Command 137
10.5.1 Enable frame delay measurement function 137
10.5.2 Show the statistics about the one-way delay measurement received locally 138
10.5.3 Show the statistical information of the Y.1731 module 139
10.5.4 Deleting the Statistics Information about the One-Way Delay Measurement Carried Out by a Designated MEG 140
10.5.5 Deleting the Transmission Statistics Information about the OAM Packets and the System Error Information 140

Chapter 11 DHCP-Relay Snooping Configuration Commands 142

11.1 ip dhcp-relay snooping 142
11.2 ip dhcp-relay snooping vlan 142
11.3 ip dhcp-relay snooping vlan *vlan_id* max-client 143
11.4 ip dhcp-relay snooping database-agent 143
11.5 ip dhcp-relay snooping db-file 144
11.6 ip dhcp-relay snooping write-time 145
11.7 ip dhcp-relay snooping write-immediately 145
11.8 ip dhcp-relay snooping log 146
11.9 ip dhcp-relay snooping rapid-refresh-bind 146
11.10 dhcp-relay snooping information option 147
11.11 ip verify source vlan 148
11.11.1 ip arp inspection vlan 148
11.12 ip source binding 149
11.13 arp inspection trust 150
11.14 dhcp snooping trust 150
11.15 dhcp snooping deny 151
11.16 dhcp snooping information circuit-id 151
11.17 dhcp snooping information remote-id string 152
11.18 dhcp snooping information vendor-specific 153

11.19 dhcp snooping information append 153
11.20 dhcp snooping information drop 154
11.21 ip-source trust 155
11.22 show ip dhcp-relay snooping 155
11.23 show ip dhcp-relay snooping binding 156
11.24 debug ip dhcp-relay snooping 156
11.25 debug ip dhcp-relay event 157
11.26 debug ip dhcp-relay binding 157

Chapter 12 DoS Attack Prevention Configuration Commands 158

12.1 dos enable 158
12.2 show dos 159

Chapter 13 EAPS Configuration Commands 161

13.1 Global Configuration Commands 161
13.1.1 ether-ring 161
13.1.2 control-vlan 161
13.1.3 master-node 162
13.1.4 transit-node 163
13.1.5 hello-time 164
13.1.6 fail-time 165
13.1.7 pre-forward-time 166
13.2 Port Configuration Commands 167
13.2.1 ether-ring primary-port 167
13.2.2 ether-ring secondary-port 168
13.2.3 ether-ring transit-port 169
13.3 Show Configuration Commands 170
13.3.1 show ether-ring 170

Chapter 14 ERPS Configuration Commands 172

14.1 Global Configuration Commands 172
14.1.1 Erps 172
14.1.2 erps nimble-mode 172
14.1.3 control-vlan 173
14.1.4 interconnection-node 174
14.1.5 raps-virtual-channel 175
14.1.6 revertive-mode 175
14.1.7 version 176
14.1.8 wtr-time 177
14.1.9 guard-time 178
14.1.10 send-time 179
14.2 Port Configuration Commands 179
14.2.1 erps ring-port 179
14.2.2 erps rpl 180
14.2.3 erps neighbor 181
14.2.4 erps mep 182
14.3 Control Commands 183
14.3.1 erps [ForcedSwitch | ManualSwitch | Clear] 183
14.4 Show Configuration Commands 184
14.4.1 show erps 184

Chapter 15 GVRP Configuration Commands 186

15.1 GVRP Configuration Commands **186**
15.1.1 GVRP 186
15.1.2 gvrp dynamic-vlan-pruning 186
15.1.3 Show gvrp statistics 187
15.1.4 Show gvrp status 188
15.1.5 Debug gvrp event 188
15.1.6 Debug gvrp packet 189
15.2 GARP Configuration Commands **189**
15.2.1 Garp timer leaveall 189
15.2.2 garp timer hold 190
15.2.3 garp timer join 191
15.2.4 garp timer leave 192
15.2.5 show garp timers 192
15.2.6 Show garp status 193
15.2.7 Debug garp 194

Chapter 16 IGMP Proxy Commands **195**

16.1 ip igmp-proxy enable **195**
16.2 ip igmp-proxy agent-vlan client-vlan map **195**
16.3 show ip igmp-proxy **196**
16.4 debug ip igmp-proxy **197**

Chapter 17 IGMP-SNOOPING Configuration Commands **199**

17.1 igmp-snooping **199**
17.2 igmp-snooping static **199**
17.3 igmp-snooping immediate-leave **200**
17.4 igmp-snooping mrouter **201**
17.5 igmp-snooping policy **202**
17.6 igmp-snooping dlf-drop **203**
17.7 igmp-snooping router age **203**
17.8 igmp-snooping response time **204**
17.9 igmp-snooping querier **204**
17.10 igmp-snooping querier querier-timer **205**
17.11 igmp-snooping forward-l3-to-mrouter **206**
17.12 igmp-snooping sensitive **206**
17.13 igmp-snooping v3-leave-check **207**
17.14 igmp-snooping forward-wrongiif-within-vlan **208**
17.15 igmp-snooping filter **208**
17.16 igmp-snooping vlan filter **209**
17.17 igmp-snooping limit **210**
17.18 igmp-snooping report-suppression **211**
17.19 igmp-snooping proxy-leave **211**
17.20 show ip igmp-snooping **212**
17.21 show ip igmp-snooping timer **213**
17.22 show ip igmp-snooping groups **214**
17.23 show ip igmp-snooping group interface **214**
17.24 show ip igmp-snooping statistics **215**
17.25 show ip igmp-snooping vlan **217**
17.26 debug ip igmp-snooping packet **218**
17.27 debug ip igmp-snooping timer **218**
17.28 debug ip igmp-snooping event **219**
17.29 debug ip igmp-snooping error **219**

17.30 debug ip igmp-snooping 220

Chapter 18 Interface Configuration Commands 221

18.1 interface 221
18.2 description 221
18.3 bandwidth 222
18.4 delay 223
18.5 shutdown 223
18.6 show interface 224
18.7 show running-config interface 225
18.8 show cable interface 226
18.9 Configuration Example 227

Chapter 19 Interface Physical Characteristic Configuration Commands 229

19.1 speed 229
19.2 duplex 229
19.3 flow-control 230

Chapter 20 Interface Range Command 232

20.1 Interface Range 232

Chapter 21 Configuring Physical Interface IP Access List Command 233

21.1 ip access-group 233
21.2 ipv6 access-group 234

Chapter 22 IP Hardware Subnet Routing Configuration Commands 236

22.1 ip exf 236
22.2 ip exf down-up-threshold 236
22.3 debug ip exf 237

Chapter 23 IP-Attack Prevention Configuration Commands 239

23.1 IP-Attack Prevention Configuration Commands 239
23.1.1 ip verify icmp ping-flood 239
23.1.2 ip verify icmp ping-sweep 239
23.1.3 ip verify tcp syn-flood 240
23.1.4 ip verify tcp syn-sweep 241
23.1.5 ip verify tcp fin-scan 241
23.1.6 ip verify tcp rst-flood 242
23.1.7 ip verify udp udp-flood 243
Syntax 243
23.1.8 ip verify udp udp-sweep 243
23.1.9 ip verify attack Xmas-Tree 244
23.1.10 ip verify attack Null-scan 245
23.1.11 ip verify attack Land 246
23.1.12 ip verify attack Smurf 246
23.1.13 ip verify attack WinNuke 247
23.1.14 ip verify attack TearDrop 248
23.1.15 ip verify attack Fraggle 248
23.1.16 ip verify all 249
23.1.17 ip verify filter 250
23.1.18 ip verify enable 251
23.1.19 ip verify log-enable 251

23.1.20 show ip table 252
23.1.21 show ip table src 252

Chapter 24 IP Direct Network Segment Scanning Attack Protection Configuration Commands 253

24.1 IP Direct Network Segment Scanning Attack Protection Configuration Commands 253
24.1.1 ip verify ip-sweep detect unknown-host 253
24.1.2 ip verify ip-sweep action rate-limit 253
24.1.3 ip verify ip-sweep action rate-limit-attacker 254
24.1.4 ip verify ip-sweep action no-cache 255
24.1.5 show ip verify config 255
24.1.6 show ip verify status 256

Chapter 25 IP-PBR Configuration Commands 257

25.1 ip pbr 257
25.2 show ip pbr 257
25.3 show ip pbr policy 258
25.4 show ip pbr exf 259
25.5 debug ip pbr 259

Chapter 26 IPv6 ACL Configuration Commands 261

26.1 IPv6 ACL Configuration Commands 261
26.1.1 ipv6 access-list 261
26.1.2 ipv6 access-group 262
26.1.3 deny/permit 263
26.1.4 Sequence 270
26.1.5 show ipv6 access-list 273

Chapter 27 IPv6 Configuration Commands 275

27.1 ipv6 address 275
27.2 ipv6 address anycast 276
27.3 ipv6 address autoconfig 277
27.4 ipv6 address eui-64 277
27.5 ipv6 address link-local 278
27.6 ipv6 enable 279
27.7 show ipv6 interface 280

Chapter 28 IPv6 Configuration Commands 282

28.1 clear ipv6 traffic 282
28.2 debug ipv6 packet 283
28.3 ipv6 mtu 284
28.4 ipv6 redirects 285
28.5 ipv6 access-group 285
28.6 ipv6 unreachables 286
28.7 ipv6 route default 287
28.8 show ipv6 general-prefix 288
28.9 show ipv6 pmtu 288
28.10 show ipv6 traffic 289
28.11 Network Test Tools Commands 291
28.11.1 ping6 291
28.12 traceroute6 293

Chapter 29 Layer-2 Tunneling Protocol Configuration Commands 295

29.1 l2protocol-tunnel **295**
29.2 no spanning-tree **295**

Chapter 30 LLDP Configuration Commands **297**

30.1 LLDP Commands **297**
30.1.1 lldp run 297
30.1.2 lldp holdtime 297
30.1.3 lldp timer 298
30.1.4 lldp reinit 299
30.1.5 lldp tlv-select 299
30.1.6 lldp dot1-tlv-select 300
30.1.7 lldp dot3-tlv-select 301
30.1.8 lldp med-tlv-select 302
30.1.9 lldp transmit 303
30.1.10 lldp receive 304
30.1.11 lldp management-ip 304
30.1.12 lldp trap-send 305
30.1.13 location elin identifier id WORD 306
30.1.14 location civic identifier id 306
30.1.15 location elin/civic id 308
30.1.16 show lldp errors 309
30.1.17 show lldp interface 310
30.1.18 show lldp neighbors 310
30.1.19 show lldp neighbors detail 311
30.1.20 show lldp traffic 312
30.1.21 show location elin 313
30.1.22 show location civic [identifier *id*] 314
30.1.23 clear lldp counters 315
30.1.24 clear lldp table 316

Chapter 31 Loopback Detection Configuration Commands **317**

31.1 loopback-detection **317**
31.2 loopback-detection enable **317**
31.3 loopback-detection vlan-control **318**
31.3.1 loopback-detection hello-time 318
31.3.2 loopback-detection recovery-time 319
31.3.3 loopback-detection delay-time 319
31.3.4 loopback-detection control 320
31.3.5 loopback-detection frames-threshold 321
31.3.6 loopback-detection frames-monitor 322
31.3.7 loopback-detection dest-mac 322
31.3.8 loopback-detection existence 323
31.3.9 loopback-detection forbid-packet 324
31.3.10 loopback-detection vlan-recovery 324
31.3.11 show loopback-detection 324
31.3.12 show loopback-detection 326

Chapter 32 MAC Access List Configuration Commands **327**

32.1 mac access-list **327**
32.2 permit **327**
32.3 deny **328**
32.4 mac access-group **329**

Chapter 33 MAC Address Configuration Commands 331

33.1 mac address-table static 331
33.2 mac address-table aging-time 331
33.3 mac address-table blackhole 332
33.4 show mac address-table 333
33.5 clear mac address-table 334

Chapter 34 MACFF Configuration Commands 335

34.1 macff enable 335
34.2 macff vlan *vlan_id* enable 335
34.3 macff vlan *vlan_id* default-ar *A.B.C.D* 336
34.4 macff vlan *vlan_id* enable other-ar *A.B.C.D* 337
34.5 macff disable 337
34.6 debug macff 338

Chapter 35 LACP MAD Configuration Commands 339

35.1 multi-active-detection 339
35.2 multi-active-relay 339

Chapter 36 MEAPS Configuration Commands 341

36.1 Global Configuration Commands 341
36.1.1 mether-ring id1 domain id2 341
36.1.2 master-node 341
36.1.3 transit-node 342
36.1.4 edge-node 343
36.1.5 assistant-node 344
36.1.6 major-ring 345
36.1.7 sub-ring 346
36.1.8 control-vlan 347
36.1.9 single-subring-mode 348
36.1.10 hello-time 348
36.1.11 fail-time 349
36.1.12 pre-forward-time 350
36.2 Port Configuration Commands 351
36.2.1 mether-ring id1 domain id2 primary-port 351
36.2.2 mether-ring id1 domain id2 secondary-port 352
36.2.3 mether-ring id1 domain id2 transit-port 353
36.2.4 mether-ring id1 domain id2 common-port 354
36.2.5 mether-ring id1 domain id2 edge-port 355
36.3 Show Configuration Commands 356
36.3.1 show mether-ring 356

Chapter 37 MLD Multicast Configuration Commands 358

37.1 ipv6 mld-snooping 358
37.2 ipv6 mld-snooping solicitation 358
37.3 ipv6 mld-snooping vlan vlan_id static X:X:X:X::X interface intf_name 359
37.4 ipv6 mld-snooping timer router-age *timer_value* 359
37.5 ipv6 mld-snooping timer response-time *timer_value* 360
37.6 ipv6 mld-snooping querier 361
37.7 ipv6 mld-snooping vlan *vlan_id* mrouter interface *inft_name* 361
37.8 ipv6 mld-snooping vlan *vlan_id* immediate-leave 362

37.9 show ipv6 mld-snooping 363
37.10 show ipv6 mld-snooping vlan vlan_id 364
37.11 show ipv6 mld-snooping timer 364
37.12 show ipv6 mld-snooping groups 365
37.13 show ipv6 mld-snooping statistics 366
37.14 show ipv6 mld-snooping mac 366

Chapter 38 Basic Multicast Commands 368

38.1 debug ip mpacket 368
38.2 debug ip mroute-cache 369
38.3 debug ip multicast 369
38.4 ip multicast-statistic 371
38.5 ip multicast-routing 371
38.6 ip multicast route-limit 372
38.7 ip multicast boundary 373
38.8 ip multicast helper-map 374
38.9 ip multicast ttl-threshold 376
38.10 show ip mroute-cache 376
38.11 show ip mroute mfc 377

Chapter 39 IGMP Configuration Commands 379

39.1 clear ip igmp group 379
39.2 debug ip igmp 379
39.3 debug ip igmp-host 380
39.4 ip igmp helper-address 381
39.5 ip igmp join-group 381
39.6 ip igmp immediate-leave group-list 382
39.7 ip igmp last-member-query-interval 383
39.8 ip igmp querier-timeout 384
39.9 ip igmp query-interval 385
39.10 ip igmp query-max-response-time 386
39.11 ip igmp static-group 387
39.12 ip igmp version 387
39.13 show ip igmp groups 388
39.14 show ip igmp interface 391
39.15 show ip igmp-host 392

Chapter 40 PIM-DM Configuration Commands 394

40.1 clear ip mroute pim-dm 394
Syntax 394
40.1.1 debug ip pim-dm 395
40.2 ip pim-dm 397
40.3 ip pim-dm dr-priority 398
40.4 ip pim-dm hello-interval 399
40.5 ip pim-dm state-refresh origination-interval 400
40.6 ip pim-dm neighor-filter 401
40.6.1 show ip pim-dm neighbor 401
40.6.2 show ip pim-dm interface 403
40.6.3 show ip rpf pim-dm 404

Chapter 41 PIM-SM Configuration Commands 406

41.1 ip pim-sm 406

41.1.1 ip pim-sm admin-scope 407
41.1.2 ip pim-sm asrt-hold 408
41.1.3 ip pim-sm bsr-border 408
41.1.4 ip pim-sm dr-pri 409
41.1.5 ip pim-sm hello-intvl 410
41.1.6 ip pim-sm holdtime 411
41.1.7 ip pim-sm horizon-split 412
41.1.8 ip pim-sm jp-hold 413
41.1.9 ip pim-sm jp-intvl 414
41.1.10 ip pim-sm lan-delay 414
41.1.11 ip pim-sm nbma-mode 415
41.1.12 ip pim-sm nbr-filter 417
41.1.13 ip pim-sm nbr-track 418
41.1.14 ip pim-sm override 419
41.1.15 router pim-sm 420
41.1.16 hello-option 421
41.1.17 accept bsm-adv 422
41.1.18 accept crp-adv 423
41.1.19 accept rp-addr 424
41.1.20 accept register 426
41.1.21 anycast-rp 427
41.1.22 reg-rate-limit 429
41.1.23 reg-src 430
41.1.24 spt-threshold 431
41.1.25 ssm 432
41.1.26 c-bsr intf_type intf_name 433
41.1.27 c-bsr admin-scope 435
41.1.28 bsm-policy 436
41.1.29 static-rp 437
41.1.30 c-rp intf_type intf_name 438
41.1.31 intvl-time 440
41.1.32 holdtime 441
41.1.33 log 443
41.1.34 clear ip pim-sm rp-mapping 444
41.1.35 clear ip mroute pim-sm 445
41.1.36 show running-configure 445
41.1.37 show ip pim-sm bsr-router 446
41.1.38 show ip pim-sm sz-info 447
41.1.39 show ip pim-sm interface 448
41.1.40 show ip pim-sm neighbor 451
41.1.41 show ip pim-sm rp 452
41.1.42 show ip pim-sm rp-hash 454
41.1.43 show ip pim-sm anycast-rp 455
41.1.44 show ip pim-sm protocol 456
41.1.45 show ip mroute pim-sm 457
41.1.46 show ip rpf pim-sm 459
41.1.47 debug ip pim-sm alert 460
41.1.48 debug ip pim-sm assert 461
41.1.49 debug ip pim-sm bsr 462
41.1.50 debug ip pim-sm rp 462
41.1.51 debug ip pim-sm entry 463
41.1.52 debug ip pim-sm event 463

41.1.53 debug ip pim-sm hello 464
41.1.54 debug ip pim-sm jp 465
41.1.55 debug ip pim-sm nbr 465
41.1.56 debug ip pim-sm packet 466
41.1.57 debug ip pim-sm register 466
41.1.58 debug ip pim-sm timer 467

Chapter 42 ND Commands 469

42.1 debug ipv6 nd 469
42.2 show ipv6 neighbors 469
42.3 clear ipv6 neighbors 470
42.4 ipv6 neighbor 470

Chapter 43 Network Management Configuration Commands 472

43.1 snmp-server community 472
43.2 snmp-server contact 473
43.3 snmp-server engineID local 474
43.4 snmp-server group 474
43.5 snmp-server [host|hostv6] 476
43.6 snmp-server location 477
43.7 snmp-server packetsize 478
43.8 snmp-server queue-length 479
43.9 snmp-server trap-source 480
43.10 snmp-server trap-timeout 480
43.11 snmp-server user 481
43.12 snmp-server view 482
43.13 snmp-server source-addr 484
43.14 snmp-server udp-port 484
43.15 snmp-server encryption 485
43.16 snmp-server trap-add-hostname 486
43.17 snmp-server trap-logs 486
43.18 snmp-server set-snmp-dos-max 487
43.19 snmp-server keep-alive 488
43.20 snmp-server necode 489
43.21 snmp-server event-id 489
43.22 snmp-server getbulk-timeout 490
43.23 snmp-server getbulk-delay 491
43.24 show snmp 491
43.25 debug snmp 494
43.26 rmon alarm 497
43.27 rmon event 498
43.28 rmon collection stats 499
43.29 rmon collection history 500
43.30 show rmon 501

Chapter 44 IP Address Configuration Commands 502

44.1 Arp static 502
44.2 arp timeout scan_intervel 503
44.3 arp timeout stale_threshold 503
44.4 arp timeout pending_timeout 504
44.5 arp timeout dynamic_arp_mac_check_enable 505
44.6 arp timeout mac_check_interval 506

44.7 clear arp 506
44.8 ip address 507
44.9 show arp 508
44.10 show arp statistics 509
44.11 show arp timeout 510
44.12 show ip interface 511
44.13 show ip cache 511

Chapter 45 NTP Configuration Commands 513

45.1 ntp master 513
45.2 ntp client 513
45.3 ntp authentication enable 514
45.4 ntp authentication key 515
45.5 ntp authentication trusted-key 516
45.6 ntp server 516
45.7 ntp peer 517
45.8 show ntp 518
45.9 debug ntp 520
45.10 time-zone 521
45.11 summer-time 522

Chapter 46 OAM Configuration Commands 524

46.1 ethernet oam 524
46.2 ethernet oam {max-rate | min-rate | mode | timeout } 524
46.3 ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action 525
46.4 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high 526
46.5 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low 527
46.6 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window 528
46.7 ethernet oam link-monitor high-threshold action 529
46.8 ethernet oam link-monitor negotiation-supported 529
46.9 clear ethernet oam statistics 530
46.9.1 show ethernet oam discovery 531
46.10 show ethernet oam statistics {pdu | link-monitor | remote-failure} 532
46.11 show ethernet oam configuration 534
46.12 show ethernet oam runtime 536

Chapter 47 Optical Port Additional Function Configuration Commands 538

47.1 Configure the DDM Function 538
47.1.1 ddm enable 538
47.1.2 no ddm 538
47.2 Configure the single-fiber transceiver function of the optical port 539
47.2.1 single-fiber one-way 539
47.3 Optical module auto-configuration 539
47.3.1 fiber-auto-config 539

Chapter 48 OSPFv3 Configuration Commands 542

48.1 area default-cost 542
48.2 area nssa 543
48.3 area range 544
48.4 area stub 545
48.5 area virtual-link 546
48.6 debug ipv6 ospf 548

48.7 debug ipv6 ospf events 550
48.8 debug ipv6 ospf ifsm 552
48.9 debug ipv6 ospf lsa 554
48.10 debug ipv6 ospf nfsm 557
48.11 debug ipv6 ospf nsm 559
48.12 debug ipv6 ospf packet 560
48.13 debug ipv6 ospf route 563
48.14 default-information originate 565
48.15 default-metric 566
48.16 filter 567
48.17 ipv6 ospf area 568
48.18 ipv6 ospf cost 569
48.19 ipv6 ospf database-filter all out 569
48.20 ipv6 ospf dead-interval 570
48.21 ipv6 ospf hello-interval 571
48.22 ipv6 ospf mtu-ignore 572
48.23 ipv6 ospf neighbor 573
48.24 ipv6 ospf network 574
48.25 ipv6 ospf priority 574
48.26 ipv6 ospf retransmit-interval 575
48.27 ipv6 ospf transmit-delay 576
48.28 passive-interface 577
48.29 redistribute 578
48.30 router ospfv3 579
48.31 router-id 579
48.32 show ipv6 ospf 580
48.33 show ipv6 ospf database 582
48.34 show ipv6 ospf interface 584
48.35 show ipv6 ospf neighbor 586
48.36 show ipv6 ospf route 587
48.37 show ipv6 ospf virtual-link 588
48.38 summary-prefix 590
48.39 timers delay 591
48.40 timers hold 591
48.41 timers age 592

Chapter 49 PDP Configuration Commands 594

49.1 pdp timer 594
49.2 pdp holdtime 594
49.3 pdp version 595
49.4 pdp run 595
49.5 pdp enable 596
49.6 show pdp traffic 596
49.7 show pdp neighbor 597

Chapter 50 Port Additional Characteristics Configuration Commands 598

50.1 Configuring Port Isolation 598
50.1.1 port-protected 598
50.1.2 description 598
50.1.3 switchport protected 599
50.2 Configuring Storm-control 600
50.2.1 storm-control 600

50.2.2 storm-control mode 600
50.2.3 storm-control action 601
50.2.4 storm-control auto-resume 602
50.2.5 storm-control notify 603
50.3 Configuring Switchport Rate-limit 603
50.4 Configuring Port Loop Check 604
50.5 Configuring Port MAC-address learning 605
50.6 Configuring Port Security 605
50.6.1 switchport port-security mode 605
50.6.2 switchport port-security dynamic 606
50.6.3 switchport port-security static mac-address 606
50.6.4 switchport port-security sticky 607
50.7 Configuring Port Binding 608
50.8 Configuring SVL/IVL 608
50.9 Configuring Link Scan 609
50.10 Configuring Port Enhanced Link Status Check 609
50.11 Configuring System mtu 610

Chapter 51 Configuring Port Mirroring Commands 611

51.1 mirror 611
51.2 show mirror 612

Chapter 52 Power Over Ethernet Configuration Commands 613

52.1 POE Configuration Commands 613
52.1.1 show poe system 613
52.1.2 show poe all 614
52.1.3 show poe power 615
52.1.4 show poe interface 617
52.1.5 poe disable 619
52.1.6 poe max-power 620
52.1.7 poe priority 620
52.1.8 poe PD-discription 621
52.1.9 poe force-power 622
52.1.10 poe inrush 622
52.1.11 poe extern-power 623
52.1.12 poe perpetual 624
52.1.13 poe detection 624

Chapter 53 Private VLAN Configuration Commands 626

53.1 private-vlan 626
53.2 private-vlan association 627
53.3 switchport mode private-vlan 627
53.4 switchport private-vlan host-association 628
53.5 switchport private-vlan mapping 629
53.6 switchport private-vlan 630
53.7 show vlan private-vlan 631
53.8 show vlan private-vlan interface 631

Chapter 54 QoS Configuration Commands 633

54.1 cos default 633
54.2 cos map 633
54.3 dscp map 634

54.4 scheduler weight bandwidth 635
54.5 scheduler policy 636
54.6 policy-map 637
54.7 classify 637
54.8 action 639
54.9 qos policy 640
54.10 show policy-map 641
54.11 trust 641

Chapter 55 VRRP Configuration Commands 643

55.1 vrrp associate 643
55.2 vrrp authentication 643
55.3 vrrp description 644
55.4 vrrp preempt 645
55.5 vrrp preempt delay 646
55.6 vrrp priority 646
55.7 vrrp source-mac-use-system 647
55.8 vrrp timers 647
55.9 vrrp track 648
55.10 show vrrp 650
55.11 debug vrrp 651

Chapter 56 RNP Configuration Commands 652

56.1 bvss rnp old-master-timeout 652
56.2 show bvss rnp 652

Chapter 57 VRF Configuration Commands 654

57.1 ip vrf vrf-name 654
57.2 description 654
57.3 export map 655
57.4 import map 656
57.5 rd 657
57.6 route-target 658
57.7 ip vrf forwarding 660
57.8 ip vrf sitemap 661
57.9 show ip vrf 662

Chapter 58 Static Route Configuration Commands 664

58.1 ip route default 664
58.2 ip route A.B.C.D 665
58.3 ip route vrf 666
58.4 ip route bfd 668
58.5 ip route load-balance 669
58.6 ip route-weight 670
58.7 ip route max-number 671
58.8 ip route max-paths static 671
58.9 show ip route 672
58.10 show ip fib 673
58.11 debug ip routing 674

Chapter 59 RIP Configuration Commands 676

59.1 auto-summary 676

59.2 default-information originate 676
59.3 default-metric 677
59.4 ip rip authentication 678
59.5 ip rip md5-key 679
59.6 ip rip dynamic-key 680
59.7 ip rip password 681
59.8 ip rip passive 682
59.9 ip rip deaf 683
59.10 ip rip receive version 683
59.11 ip rip send version 684
59.12 ip rip v1demand 685
59.13 ip rip v2demand 686
59.14 ip rip split-horizon 687
59.15 ip rip process-id enable 688
59.16 neighbor 689
59.17 offset 689
59.18 router rip process-id 690
59.19 timers expire 691
59.20 timers holddown 692
59.21 timers update 693
59.22 timers trigger 694
59.23 timers peer 694
59.24 validate-update-source 695
59.25 check-zero-domain 696
59.26 version 696
59.27 distance 697
59.28 filter 698
59.29 maxinum-nexthop 699
59.30 input-queue 700
59.31 show ip rip 700
59.32 show ip rip process-id interface 702
59.33 show ip rip process-id summary 703
59.34 show ip rip process-id database 704
59.35 show ip rip process-id protocol 705
59.36 show ip rip process-id peer 706
59.37 debug ip rip database 706
59.38 debug ip rip packet [send | receive] 707
59.39 debug ip rip message 708

Chapter 60 BEIGRP Configuration Commands 710

60.1 auto-summary 710
60.2 clear ip beigrp neighbors 710
60.3 debug ip beigrp 711
60.4 debug ip beigrp fsm 711
60.5 debug ip beigrp neighbors 712
60.6 debug ip beigrp transmit 715
60.7 default-metric 715
60.8 Distance 716
60.9 Filter 718
60.10 beigrp log-neighbor-changes 719
60.11 beigrp router-id 719
60.12 ip beigrp bandwidth-percent 720

60.13 ip beigrp hello-interval 721
60.14 ip beigrp hold-time 721
60.15 ip beigrp passive 722
60.16 ip beigrp split-horizon 723
60.17 metric weights 723
60.18 Network 724
60.19 Offset 725
60.20 redistribute 726
60.21 router beigrp 727
60.22 show ip beigrp interface 728
60.23 show ip beigrp neighbors 729
60.24 show ip beigrp protocol 730
60.25 show ip beigrp topology 731
60.26 show ip beigrp traffic 733

Chapter 61 OSPF Configuration Commands 735

61.1 area authentication 735
61.2 area default-cost 736
61.3 area filter 737
61.4 area nssa 739
61.5 area nssa-range 740
61.6 area nssa-translate-interval 742
61.7 area range 743
61.8 area stub 745
61.9 area virtual-link 746
61.10 auto-cost 748
61.11 bfd all-interfaces 749
61.12 debug ip ospf adj 750
61.13 debug ip ospf events 751
61.14 debug ip ospf flood 753
61.15 debug ip ospf lsa-generation 754
61.16 debug ip ospf packet 755
61.17 debug ip ospf restart 756
61.18 debug ip ospf retransmission 758
61.19 debug ip ospf spf 758
61.20 debug ip ospf tree 760
61.21 default-information originate 761
61.22 default-metric 762
61.23 distance 763
61.24 distance ospf 764
61.25 filter 765
61.26 graceful-restart 766
61.27 ip ospf authentication 767
61.28 ip ospf bfd 768
61.29 ip ospf cost 769
61.30 ip ospf dead-interval 770
61.31 ip ospf demand-circuit 771
61.32 ip ospf hello-interval 771
61.33 ip ospf message-digest-key 772
61.34 ip ospf mib-binding 774
61.35 ip ospf network 775
61.36 ip ospf passive 775

61.37 ip ospf password 776
61.38 ip ospf priority 777
61.39 ip ospf retransmit-interval 778
61.40 ip ospf transmit-delay 778
61.41 ip ospf mtu-ignore 779
61.42 limit max-ext-lsa 779
61.43 limit retransmissions 780
61.44 maximum-paths 781
61.45 neighbor 782
61.46 network area 783
61.47 redistribute 784
61.48 restart ospf 785
61.49 router-id 786
61.50 router ospf 787
61.51 show ip ospf 787
61.52 show ip ospf border-routers 789
61.53 show ip ospf database 790
61.54 show ip ospf interface 792
61.55 show ip ospf neighbor 793
61.56 show ip ospf virtual-link 794
61.57 stub-router 795
61.58 summary-address 796
61.59 timers delay-timer 797
61.60 timers hold-timer 798
61.61 timers age-timer 798

Chapter 62 BGP Configuration Commands 800

62.1 address-family ipv4 800
62.2 address-family ipv6 801
62.3 address-family vpnv4 801
62.4 aggregate-address 802
62.5 bgp always-compare-med 804
62.6 bgp asnotation dot 804
62.7 bgp bestpath med 805
62.8 bgp client-to-client reflection 806
62.9 bgp cluster-id 807
62.10 bgp confederation identifier 808
62.11 bgp confederation peers 809
62.12 bgp dampening 810
62.13 bgp default local-preference 811
62.14 bgp default route-target filter 812
62.15 bgp deterministic-med 813
62.16 bgp fast-external-fallover 813
62.17 bgp graceful-restart 814
62.18 bgp maxas-limit 815
62.19 bgp router-id 815
62.20 bgp update-delay 816
62.21 bgp redistribute-internal 817
62.22 clear ip bgp 818
62.23 debug ip bgp 819
62.24 distance 820
62.25 filter 822

62.26 maximum-paths 823
62.27 neighbor activate 824
62.28 neighbor advertisement-interval 824
62.29 neighbor allowas-in 825
62.30 neighbor capability orf prefix-list 826
62.31 neighbor default-originate 827
62.32 neighbor description 828
62.33 neighbor distribute-list 829
62.34 neighbor ebgp-multihop 830
62.35 neighbor fall-over 831
62.36 neighbor filter-list 832
62.37 neighbor maximum-prefix 833
62.38 neighbor next-hop-self 834
62.39 neighbor password 836
62.40 neighbor peer-group 837
62.41 neighbor prefix-list 838
62.42 neighbor remote-as 839
62.43 neighbor remove-private-AS 840
62.44 neighbor route-map 841
62.45 neighbor route-reflector-client 843
62.46 neighbor route-refresh 844
62.47 neighbor send-community 845
62.48 neighbor send-label 846
62.49 neighbor shutdown 846
62.50 neighbor soft-reconfiguration 847
62.51 neighbor timers 848
62.52 neighbor ttl-security-hop 849
62.53 neighbor update-source 850
62.54 neighbor weight 851
62.55 network (BGP) 852
62.56 redistribute(BGP) 854
62.57 router bgp 855
62.58 show ip bgp 856
62.59 show ip bgp community 857
62.60 show ip bgp ipv6 unicast 858
62.61 show ip bgp neighbors 859
62.62 show ip bgp paths 860
62.63 show ip bgp prefix-list 860
62.64 show ip bgp regexp 861
62.65 show ip bgp summary 862
62.66 synchronization 863
62.67 table-map 864
62.68 timers 864

Chapter 63 Public Routing Configuration Commands 866

63.1 Ip aspath-list Configuration Commands 866
63.1.1 ip as-path access-list 866
63.2 show ip aspath-list 868
63.3 ip community-list Configuration Commands 869
63.3.1 ip community-list 869
63.3.2 show ip community-list 870
63.4 ip prefix-list commands 871

63.4.1 clear ip prefix-list 871
63.4.2 ip prefix-list 872
63.4.3 ip prefix-list description 874
63.4.4 ip prefix-list sequence-number 875
63.4.5 show ip prefix-list 875
63.5 route-map Commands 877
63.5.1 route-map 877
63.5.2 match as-path 879
63.5.3 match community 881
63.5.4 match ip address 882
63.5.5 match ip next-hop 883
63.5.6 match ip address prefix-list 885
63.5.7 match length 886
63.5.8 match metric 887
63.5.9 match tag 888
63.5.10 on-match 890
63.5.11 set aggregator 891
63.5.12 set as-path 893
63.5.13 set atomic-aggregate 894
63.5.14 set community 895
63.5.15 set community-additive 897
63.5.16 set default 899
63.5.17 set interface 899
63.5.18 set ip default 900
63.5.19 set ip precedence 901
63.5.20 set ip tos 902
63.5.21 set ip next-hop 903
63.5.22 set local-preference 904
63.5.23 set metric 905
63.5.24 set metric-type 907
63.5.25 set origin 908
63.5.26 set tag 910
63.5.27 set weight 911
63.5.28 show route-map 913

Chapter 64 PBR Configuration Commands 915

64.1 debug ip policy 915
64.2 ip policy route-map 915
64.2.1 match ip address 916
64.2.2 match length 917
64.2.3 set default interface 918
64.2.4 set interface 919
64.2.5 set ip default next-hop 920
64.2.6 set ip next-hop 921
64.2.7 route-map 922
64.2.8 ip local policy 923
64.2.9 ip policy 924
64.2.10 ip route-weight 926
64.2.11 show ip local policy 927
64.2.12 show ip policy 928

Chapter 65 Switch Routing Protocol Highpriority Configuration Commands 929

65.1 switch routing-protocol-highpriority 929

Chapter 66 AAA Configuration Commands 930

66.1 aaa authentication banner 930
66.2 aaa authentication fail-message 930
66.3 aaa authentication username-prompt 931
66.4 aaa authentication password-prompt 932
66.4.1 aaa authentication dot1x 933
66.4.2 aaa authentication enable default 935
66.4.3 aaa authentication login 936
66.4.4 aaa group server 937
66.4.5 server 938
66.4.6 debug aaa authentication 940
66.4.7 enable password 940
66.4.8 enable(enter) 941
66.4.9 service password-encryption 942
66.5 aaa authorization 943
66.6 debug aaa authorization 945
66.7 aaa accounting 946
66.8 aaa accounting update 947
66.9 aaa accounting suppress null-username 948
66.10 debug aaa accounting 948
66.11 localauthen 949
66.12 localauthor 950
66.13 localpass 951
66.14 localgroup 953
66.15 local authen-group 954
66.16 local author-group 955
66.17 local pass-group 955
66.18 local user 956
66.19 username 957
66.20 show local-users 959
66.21 show aaa users 960

Chapter 67 RADIUS Configuration Commands 962

67.1 debug radius 962
67.2 ip radius source-interface 962
67.3 radius-server attribute 963
67.4 radius-server challenge-noecho 964
67.5 radius-server deadtime 965
67.6 radius-server directed-resquest 966
67.7 radius-server host 967
67.8 radius-server key 968
67.9 radius-server optional-passwords 969
67.10 radius-server retransmit 970
67.11 radius-server timeout 970
67.12 radius-server vsa send 971
67.13 radius-server acct-on 972

Chapter 68 TACACS+ Commands 974

68.1 debug tacacs 974
68.2 p tacacs source-interface 974

68.3 tacacs-server host 975
68.4 tacacs-server key 976
68.5 tacacs-server timeout 977

Chapter 69 SGNP Configuration Commands 979

69.1 bvss sgnp neighbour-timeout 979
69.2 show bvss sgnp 979

Chapter 70 STP Configuration Commands 981

70.1 SSTP Configuration Commands 981
70.1.1 spanning-tree 981
70.1.2 spanning-tree mode sstp 981
70.1.3 spanning-tree sstp priority 982
70.1.4 spanning-tree sstp hello-time 983
70.1.5 spanning-tree sstp max-age 983
70.1.6 spanning-tree sstp forward-time 984
70.1.7 spanning-tree sstp cost 985
70.1.8 spanning-tree cost 986
70.1.9 spanning-tree sstp port-priority 986
70.1.10 spanning-tree port-priority 987
70.1.11 show spanning-tree 988
70.1.12 spanning-tree management trap 989
70.2 VLAN STP Configuration Commands 990
70.2.1 spanning-tree mode pvst 990
70.2.2 spanning-tree vlan 990
70.2.3 spanning-tree vlan priority 991
70.2.4 spanning-tree vlan forward-time 992
70.2.5 spanning-tree vlan max-age 993
70.2.6 spanning-tree vlan hello-time 993
70.2.7 spanning-tree vlan cost 994
70.2.8 spanning-tree vlan port-priority 995
70.2.9 show spanning-tree vlan 996
70.2.10 show spanning-tree pvst instance-list 997

Chapter 71 RSTP Configuration Commands 999

71.1 RSTP Configuration Commands 999
71.1.1 spanning-tree mode rstp 999
71.1.2 spanning-tree rstp forward-time 999
71.1.3 spanning-tree rstp hello-time 1000
71.1.4 spanning-tree rstp max-age 1000
71.1.5 spanning-tree rstp priority 1001
71.1.6 spanning-tree rstp cost 1002
71.1.7 spanning-tree rstp port-priority 1002
71.1.8 spanning-tree rstp edge 1003
71.1.9 spanning-tree rstp point-to-point 1004
71.1.10 spanning-tree rstp migration-check 1004

Chapter 72 MSTP Configuration Commands 1006

72.1 MSTP Configuration Command 1006
72.1.1 spanning-tree mode mstp 1006
72.1.2 spanning-tree mstp name 1006
72.1.3 spanning-tree mstp revision 1007

72.1.4 spanning-tree mstp instance 1007
72.1.5 spanning-tree mstp root 1008
72.1.6 spanning-tree mstp priority 1009
72.1.7 spanning-tree mstp hello-time 1010
72.1.8 spanning-tree mstp forward-time 1011
72.1.9 spanning-tree mstp max-age 1011
72.1.10 spanning-tree mstp diameter 1012
72.1.11 spanning-tree mstp max-hops 1013
72.1.12 spanning-tree mstp port-priority 1013
72.1.13 spanning-tree mstp cost 1014
72.1.14 spanning-tree mstp edge 1015
72.1.15 spanning-tree mstp point-to-point 1015
72.1.16 spanning-tree mstp mst-compatible 1016
72.1.17 spanning-tree mstp migration-check 1017
72.1.18 spanning-tree mstp restricted-role 1017
72.1.19 spanning-tree mstp restricted-tcn 1018
72.1.20 show spanning-tree mstp 1018
72.1.21 show spanning-tree mstp region 1020
72.1.22 show spanning-tree mstp detail 1021
72.1.23 show spanning-tree mstp interface 1023
72.1.24 show spanning-tree mstp protocol-migration 1025

Chapter 73 STP Optional Characteristic Configuration Commands 1027

73.1 STP Optional Characteristic Configuration Commands 1027
73.1.1 spanning-tree portfast 1027
73.1.2 spanning-tree bpduguard 1028
73.1.3 spanning-tree bpdufilter 1028
73.1.4 spanning-tree uplinkfast 1029
73.1.5 spanning-tree backbonefast 1029
73.1.6 spanning-tree guard 1030
73.1.7 spanning-tree loopguard 1031
73.1.8 spanning-tree loopfast 1031
73.1.9 spanning-tree fast-aging 1032
73.1.10 spanning-tree fast-aging flush-fdb 1033
73.1.11 spanning-tree bpdu-terminal 1033

Chapter 74 ime Range Configuration Commands 1035

74.1 absolute 1035
74.2 periodic 1036
74.3 show time-range 1037
74.4 time-range 1038
74.5 debug time-range 1039

Chapter 75 UDLD Configuration Commands 1041

75.1 udld enable 1041
75.2 udld aggressive 1041
75.3 udld port 1042
75.4 udld port aggressive 1042
75.5 udld message 1043
75.6 udld reset 1044
75.7 show udld 1044

Chapter 76 Urpf Configuration Commands 1048

76.1 urpf check(Global) 1048
76.2 urpf check(VLAN interface) 1048

Chapter 77 UDLD Configuration Commands 1050

77.1 udld enable 1050
77.2 udld aggressive 1050
77.3 udld port 1051
77.4 udld port aggressive 1051
77.5 udld message 1052
77.6 udld reset 1053
77.7 show udld 1053

Chapter 1 802.1x Configuration Commands

1.1 dot1x enable

Syntax

dot1x enable
no dot1x enable

Parameter

None

Default

None

Usage Guidelines

Use this command to enable 802.1x feature. The 802.1x feature cannot be enabled on an interface. If 802.1x feature is disabled, then all 802.1x packets will be forwarded like other multi-cast packets in VLAN rather than be received by CPU

Command Mode

Global Configuration Mode

Example

The following example shows how to enable dot1x:
Switch_config#dot1x enable
Switch_config #

1.2 dot1x port-control

Syntax

dot1x port-control {auto|force-authorized|force-unauthorized|misc-mab}

no dot1x port-control

Parameter

Parameter	Description
auto	Enables 802.1x protocol authentication method
force-authorized	Forced port authentication passed
force-unauthorized	Forced port authentication failed
Misc-mab	Hybrid mode for multi-user and mab authentication

Default

force-authorized

Usage Guidelines

The 802.1x protocol is an interface-based two-layer authentication mode. You can run the auto command to enable the authentication mode. This authentication mode can be configured only on the physical interface and the interface's attributes cannot include VLAN backbone, dynamical access, security port or listening port

Command Mode

Interface configuration mode

Example

The following example enables 802.1x on interface g0/1

Switch_config _g0/1# dot1x port-control auto

Switch_config _g0/1#

The following example configures interface g0/1 as the vlan trunk port and enables

802.1x:

Switch_config _g0/1#switchport mode trunk

Switch_config _g0/1#dot1x port-control auto

802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(g0/1)

Switch_config _g0/1#

1.3 dot1x authentication multiple-hosts

Syntax

dot1x authentication multiple-hosts

no dot1x authentication multiple-hosts

Parameter

None

Default

Disable the multiple authentication of 802.1x

Usage Guidelines

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. When one user passes the authentication, the port sets to the "up" state. Other users can access the port without authentication

Note: After modifying the multi-host authentication mode, all users of the port will be authenticated again

Command Mode

Interface configuration mode

Example

The following example enables multiple-hosts authentication on interface g0/1:

Switch_config _g0/1# dot1x authentication multiple-hosts

Switch_config _g0/1#

1.4 dot1x authentication multiple-auth

Syntax

dot1x authentication multiple-auth

no dot1x authentication multiple-auth

Parameter

None

Default

Disable the multiple authentication of 802.1x

Usage Guidelines

After set one interface to the multiple-auth mode of 802.1x, the switch will set authentication for each user. The authentication for each user is unrelated. The interface shows “up” only when one user is successfully authenticate; the interface shows “down” when all users fail to authenticate. Thus, each user is respectively authenticated and any user’s failure of authentication has no effect on the authority of other users

Note: The multi-auth mode cannot be configured with guest vlan, nor with mab. To modify the multi-host mode, all user need to be re-authenticated

Command Mode

Interface configuration mode

Example

The following example shows how to enable multiple-auth in interface g0/1:

Switch_config _g0/1# dot1x authentication multiple-auth

Switch_config _g0/1#

1.5 dot1x default

Syntax

dot1x default

Parameter

None

Default

None

Usage Guidelines

The command is used to return all configuration to the default setting

Command Mode

Global Configuration Mode

Example

The command shows how to return all configurations of dot1x to the default setting

Switch_config #dot1x default

Switch_config #

1.6 dot1x reauth-max

Syntax

dot1x reauth-max count

no dot1x reauth-max

Parameter

Parameter	Syntax
count	Maximum number of retries. The value is from 1 to 10

Default

5

Usage Guidelines

Use this command to set maximum number of re-authentications. The authentication will be suspended when there is no response from client on exceeding the number of this configured re-authentication times

Command Mode

Global configuration mode

Example

The following example set 4 as the maximum number of re-authentications:

Switch_config #dot1x reauth-max 4

Switch_config #

1.7 dot1x re-authentication

Syntax

dot1x re-authentication

no dot1x re-authentication

Parameter

None

Default

None

Usage Guidelines

You configure the amount of time between the periodic re-authentication attempts by using the **dot1x timeout re-authperiod** global configuration command

Command Mode

Global configuration mode

Example

This example shows how to enable the periodic re-authentication:

Switch(config)#dot1x re-authentication

Switch(config)#

1.8 dot1x timeout quiet-period

Syntax

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

Parameter

Parameter	Syntax
time	Period of re-enabling authentication, in the range from 0 to 65535 seconds

Default

60s

Usage Guidelines

There will be a period of quiet time after authentication failure during which switch doesn't receive or enable any authentication

Command Mode

Global configuration mode

Example

The following example configures quiet period value to 40:

Switch_config #dot1x timeout quiet-period 40

Switch_config #

1.9 dot1x timeout re-authperiod

Syntax

dot1x timeout re-authperiod *time*

no dot1x timeout re-authperiod

Parameter

Parameter	Description
time	Period of re-authentication, in the range from 1 to 4294967295 seconds

Default

3600s

Usage Guidelines

This command is valid only after enabling the dot1x re-authentication command

Command Mode

Global configuration mode

Example

The following example configures dot1x re-authentication period to 7200s:

Switch_config # dot1x timeout re-authperiod 7200

Switch_config #

1.9.1 dot1x timeout tx-period

Syntax

dot1x timeout tx-period *time*

no dot1x timeout tx-period

Parameter

Parameter	Description
time	Time is from 1 to 65535s.

Default

30s

Usage Guidelines

This command specifies the time interval of the host client to respond to the authentication request. The switch will resend the authentication request when exceeding this time interval

Command Mode

Global Configuration Mode

Example

The following command sets 24 as the timeout period:

Switch(config_f0/0)# dot1x timeout tx-period 24

Switch(config_f0/0)#

1.10 dot1x mab

Syntax

dot1x mab

no dot1x mab

Parameter

None

Default

Disabled

Usage Guidelines

When a peer device cannot run the 802.1x client software, the switch will adopt the MAB authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication

When MAB is enabled and the peer device, however, neither sends the eapol_start packet nor responds to the request_identity packet and exceeds the timeout threshold, the switch regards the peer device not to support the 802.1x authentication client and then turns to the MAB authentication

Note: The multi-auth mode cannot coexist with guest vlan or mab

Command Mode

Interface Configuration Mode

Example

The following example shows how to enable mab authentication in interface g0/1.

Switch_config _g0/1# dot1x mab

Switch_config _g0/1#

1.11 dot1x mabformat

Syntax

dot1x mabformat {1|2|3|4|5|6}

no dot1x mabformat

Parameter

Parameter	Description
1	MAC address format: aa:bb:cc:dd:ee:ff
2	MAC address format: AA:BB:CC:DD:EE:FF
3	MAC address format: aabbccddeeff
4	MAC address format: AABBCCDDEEFF
5	MAC address format: aa-bb-cc-dd-ee-ff
6	MAC address format: AA-BB-CC-DD-EE-FF

Default

The default is 1

Usage Guidelines

When the MAB authentication is enabled, you can set the format of the MAC address to the Radius server through this command

Command Mode

Global configuration mode

Example

The following example shows how to configure the mac format as 3

Switch_config # dot1x mabformat 3

Switch_config #

1.12 dot1x user-permit

1.12.1 dot1x user-permit

Syntax

dot1x user-permit xxx yyy zzz

no dot1x user-permit

Parameter

Parameter	Syntax
xxx	Username
yyy	Username
zzz	Username

Default

All users are allowed to pass without user-bind

Usage Guidelines

Use this command to bind user on the interface, eight users can be binded on each interface. When enabled 802.1x authentication, the authentication is only available to the binding user

Command Mode

Interface configuration mode

Example

The following example configures a,b,c,d as the binding user on interface g0/1:

Switch_config _g0/1# dot1x user-permit a b c d

Switch_config _g0/1#

1.13 1dot1x authentication method

Syntax

dot1x authentication method xxx

no dot1x authentication method

Parameter

Parameter	Description
xxx	Method name

Default

The default method

Usage Guidelines

This command is used to configure the authentication method which must be one of authentication methods provided by AAA. One interface only uses one authentication method. When AAA performs authentication to the 802.1x user, AAA would select the configured authentication method to perform the authentication

Command Mode

Interface configuration mode

Example

The following example shows that how to set the authentication method of g0/1 to abcd. The method applies the local user name to authenticate. In interface g0/2 set the authentication method to efgh. The method applies radius remote authentication

Switch_config #aaa authentication dot1x abcd local

Switch_config #aaa authentication dot1x efgh group radius

Switch_config #int g0/1

Switch_config _g0/1# dot1x authentication method abcd

Switch_config _g0/1# int g0/2

Switch_config _g0/2# dot1x authentication method efgh

1.14 dot1x accounting enable

Syntax

dot1x accounting enable

no dot1x accounting enable

Parameter

None

Default

Disabled

Usage Guidelines

Use this command to enable accounting feature on the interface. This command must combine with the authentication feature. You'd better enable dotx re-authentication feature

Command Mode

Interface Configuration Mode

Example

The following command enables the dot1x authentication and accounting feature of interface g0/1:

Switch_config #dot1x enable

Switch_config #int g0/1

Switch_config _g0/1# dot1x port auto

Switch_config _g0/1# dot1x accounting enable

1.15 dot1x accounting method

Syntax

dot1x accounting method xxx

no dot1x accounting method

Parameter

Parameter	Syntax
xxx	Accounting method name

Default

"default" method

Usage Guidelines

Use this command to configure the accounting method on an interface. This method is one of the accounting methods that AAA provides. Each interface only uses one method. When enabled dot1 accounting feature, this method will be used to perform accounting

Command Mode

Interface configuration mode

Example

The following example configures abcd as the accounting method on interface g0/1 and this method uses radius server:

Switch_config # aaa accounting network abcd start-stop group radius

Switch_config #radius host 192.168.20.100

Switch_config #int g0/1

Switch_config _g0/1# dot1x accounting method abcd

1.16 dot1x authen-type, dot1x authentication type

Syntax

dot1x authen-type {chap|eap}

no dot1x authen-type

To set the authentication type in global configuration mode, run the above command. To return to the default

setting, use the no form of this command

dot1x authentication type {chap|eap}

no dot1x authentication type

To set the authentication type in interface configuration mode, run the above command. To return to the default setting, use the no form of this command

Parameter

None

Default

Eap in global configuration mode

Default authentication type of the interface is same as in the global configuration mode

Usage Guidelines

The authentication type decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings

Command Mode

Interface and global configuration mode

Example

The following example shows how to set the authentication type on interface g0/1 to chap and the global authentication type to eap.

Switch_config #dot1x authen-type eap

Switch_config #int g0/1

Switch_config _g0/1# dot1x authentication type chap

1.17 dot1x guest-vlan

Syntax

Enable the guest-vlan feature of the dot1x with **dot1x guest-vlan** command in global configuration mode, and disable with the no form of this command

dot1x guest-vlan

no dot1x guest-vlan

Parameter

None

Default

Disable

Usage Guidelines

When you enable the guest-vlan command, the software will assign the corresponding port to a guest VLAN when it does not receive a response from the client

This command is used with the **dot 1x guest-valan** id interface configuration command

Note: This command cannot be configured with **multiple-auth** command simultaneously

Command Mode

Global configuration mode

Example

The following example enables guest-vlan feature in global configuration mode:

Switch(config) #dot1x guest-vlan

1.18 dot1x guest-vlan id

1.18.1 dot1x guest-vlan id

Syntax

To configure dot1x guest-vlan id value (range from 1 to 4094) on an interface, use the **dot1x guest-vlan** command. Use the no form of this command to restore the default value

dot1x guest-vlan id

no dot1x guest-vlan

Parameter

Id: guest vlan value, which can be any configured vlan id in the system

Default

None

Usage Guidelines

When you enable the guest-vlan command, the software will assign the corresponding port to a guest VLAN when it does not receive a response from the client

This command is used with the **dot1x guest-vlan** global configuration command

Note: This command cannot be configured with **multiple-auth** command simultaneously

Command Mode

Interface configuration mode

Example

The following example configures guest-vlan id value on the interface g0/1:

Switch_config _g0/1#dot1x guest-vlan 2

1.19 dot1x forbid multi-network-adapter

Syntax

To forbid the supplicant of the multi-network-adapter, use the **dot1x forbid multi-network-adapter** command. Use no form of this command to restore the default configuration

dot1x forbid multi-network-adapter

no dot1x forbid multi-network-adapter

Parameter

None

Default

None

Usage Guidelines

Use this command to forbid the supplicant of the multi-network-adapter to avoid occurrence of the agent

Command Mode

Interface configuration mode

Example

The following example forbids the supplicant of the multi-network-adapter on the interface g0/1:

Switch_config _g0/1 # dot1x forbid multi-network-adapter

1.20 dot1x keepalive

Syntax

dot1x keepalive

no dot1x keepalive

To enable/disable the keepalive detection for the authentication user in the global configuration mode, run the above commands

Parameter

None

Default

Enable

Usage Guidelines

The default is to enable the keepalive detection

Command Mode

Global configuration mode

Example

The following example shows how to disable the keepalive function

Switch_config #no dot1x keepalive

Switch_config #

1.21 aaa authentication dot1x

Syntax

aaa authentication dot1x *{default | word } method1 [method2...]*

no aaa authentication dot1x *{ default | word}*

Parameter

Parameter	Syntax
default	Default authentication method. Use this authentication method when you do not specify the authentication method using the **dot1x authentication method** command
word	Designate the name of the authentication method
method1 *[method2...]*	group radius/tacacs+/xxx、local、local-case、none

Default

None

Usage Guidelines

The method parameter identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. It is best to use radius authentication for the 802.1X aaa authentication, or you can use local configuration data for authentication, such as the user password stored locally in the configuration

Command Mode

Global configuration mode

Example

The following example configures RADIUS as the dot1x authentication method:

Switch_config #aaa authentication dot1x default group radius

Switch_config #

1.22 debug dot1x errors

Syntax

debug dot1x errors

Parameter

None

Default

None

Usage Guidelines

This command is used to debug all error information during dot1x running to locate errors

1.23 debug dot1x state

Syntax

debug dot1x state

Parameter

None

Default

None

Usage Guidelines

Output format is as follows:

2003-3-18 17:40:09 802.1x:AuthSM(G0/1) state Connecting-> Authenticating, event rxRespId

2003-3-18 17:40:09 802.1x:G0/1 Create user for Enter authentication

2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Idle-> Response, event authStart

2003-3-18 17:40:09 802.1x:G0/1 user "myname" denied, Authentication Force Failed

2003-3-18 17:40:09 802.1x:G0/1 Authentication Fail

2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Response-> Fail, event aFail

1.24 debug dot1x packet

Syntax

debug dot1x packet

Parameter

None

Default

None

Usage Guidelines

2003-3-18 17:40:09 802.1xG0/1 Tx --> Supplicant(0008.74bb.d21f)

EAPOL ver:01, type:00, len:5

EAP code:01, id:03, type:01, len:5

00

2003-3-18 17:40:09 802.1x:G0/1 Rx <-- Supplicant(0008.74bb.d21f)

EAPOL ver:01, type:00, len:10

EAP code:02, id:03, type:01, len:10

62 64 63 6f 6d a5

1.25 show dot1x

Syntax

To show 802.1x configuration information, use the **show dot1x** command

show dot1x *[interface intf-id | statistics|misc-mab-db]*

Parameter

Parameter	Description
interface	Shows the dot1x interface information
intf-id	The concrete physical interface.
statistics	Shows the dot1x statistics information
misc-mab-db	Shows the dot1x mixing Mab statistics information

Default

None

Usage Guidelines

This command is used to show 802.1x configuration information

Command Mode

EXEC or configuration mode

Example

The following example shows how to display 802.1x configuration information:

Switch_config#show dot1x

802.1X Parameters

reAuthen No

reAuth-Period 3

quiet-Period 10

Tx-Period 30

Supp-timeout 30

Server-timeout 30

reAuth-max 4

max-request 2

authen-type Eap

IEEE 802.1x on port G0/1 enabled

Authorized Yes

Authen Type Eap

Authen Method default

Permit Users All Users

Multiple Hosts Disallowed

Supplicant aaa(0008.74bb.d21f)

Current Identifier 21

Authenticator State Machine

State Authenticated

Reauth Count 0

Backend State Machine

State Idle

Request Count 0

Identifier (Server) 20

Port Timer Machine

Auth Tx While Time 16

Backend While Time 16

reAuth Wait Time 3

Hold Wait Time 0

Chapter 2 Anti-Attack Configuration Commands

2.1 Anti-AttaAnti-Attack Configuration Commands

2.1.1 filter period

Syntax

To configure filter period for attack, use the filter period command

filter period *time*

To configure the attack checkup period, run the following command

no filter period

Parameter

Parameter	Description
time	The filter period for attack in seconds. It is considered as attack when the attack source sends packets above the specified number in any filter period time Value range: 1-600s

Default

10 seconds

Command Mode

Global configuration mode

Example

Switch_config# filter period 15

Related Command

filter threshold

2.1.2 filter threshold

Syntax

To configure the filter threshold value, use the filter threshold value command. Vary your configuration in terms of the packet type

filter threshold *type value*

To resume to the default value, use the no form of the previous command

no filter threshold *type*

Parameter

Parameter	Description
type	Packet type, including ARP, BPDU, DHCP, IGMP, ICMP, IP
value	It is considered as attack when the receiving packets excddes the filter threshold value. Value range: 5-2000

Default

1000

Command Mode

Global configuration mode

Example

Switch_config# filter threshold ip 1500

Related Command

filter period

2.1.3 filter block-time

Syntax

To configure the time to block attack resource, use the filter block-time value command

filter block-time *value*

To resume to the default value, use the no form of this command

no filter block-time

Parameter

Parameter	Description
Value	Time to block attack source in seconds Value range: 1-86400

Default

300 seconds

Command Mode

Global configuration mode

Example

Switch_config# filter block-time 600

Related Command

filter period

filter threshold

2.1.4 filter polling period

Syntax

To configure the period of the attack source polling check in the hybrid mode, run the following command.

filter polling period *time*

To resume to the default value, use the no form of the previous command

no filter polling period

Parameter

Parameter	Description
time	The period of the polling attack after blocking the attack source. Unit: second Value range: 1-600

Default

10s

Command Mode

Global configuration mode

Example

Switch_config# filter polling period 20

Related Command

filter polling threshold

filter polling auto-fit

2.1.5 filter polling threshold

Syntax

To configure the filter polling threshold in the hybrid mode, run the following command

filter polling thredhold *type value*

To resume to the default value, use the no form of the previous command

no filter polling threshold *type*

Parameter

Parameter	Description
type	The packet type, including ARP, BPDU, DHCP, IGMP, ICMP, IP
value	The attack source is taken as existed if 1-2000 packets are received within any polling period Value range: 1-2000

Default

750 packets

Command Mode

Global configuration mode

Example

Switch_config# filter polling threshold ip 1500

Related Commands

filter polling period

filter polling auto-fit

2.1.6 filter polling auto-fit

Syntax

To configure auto-fit the polling detect period and thereshold, run the following command. The command is efficient by default. The polling period equals with the attack detection period and the polling packet threshold equals to 3/4 of the attack detection packet threshold

filter polling auto-fit

To resume to the default setting, use the no form of this command

no filter polling auto-fit

Parameter

None

Command Mode

Global configuration mode

Example

Switch_config# filter polling auto-fit

Related Commands

filter polling period

filter polling threshold

2.1.7 filter igmp

Syntax

To enable IGMP attack detection, run the following command

ilter igmp

To disable IGMP attack detection, run the no form of the previous command

no filter igmp

Parameter

None

Command mode

Global configuration mode

Example

Switch_config# filter igmp

Related command

filter enable

2.1.8 filter ip source-ip

Syntax

To enable IP attack detection, run the following command

filter ip source-ip

To disable IP attack detection, run the no form of the previous command

no filter ip source-ip

Parameter

None

Command mode

Global configuration mode and physical port configuration mode

The command is efficient when both the global port and the physical port are configured

Example

Switch_config# filter ip source-ip

Switch_config# interface g0/1

switch_config_g0/1# filter ip source-ip

Related command

filter enable

2.1.9 filter icmp

Syntax

To enable ICMP attack detection, run the following command

filter icmp

To disable ICMP attack detection, run the no form of the previous command

no filter icmp

Parameter

None

Command mode

Global configuration mode and physical port configuration mode

The command is efficient when both the global port and the physical port are configured

Example

Switch_config# filter icmp

Switch_config# interface g0/1

switch_config_g0/1# filter icmp

Related command

filter enable

2.1.10 filter icmpv6

Syntax

To enable ICMPv6 attack detection, run the following command

filter icmpv6

To disable ICMPv6 attack detection, run the no form of the previous command

no filter icmpv6

Parameter

None

Command mode

Global configuration mode and physical port configuration mode

The command is efficient when both the global port and the physical port are configured

Example

Switch_config# filter icmpv6

Switch_config# interface g0/1

switch_config_g0/1# filter icmpv6

Related command

filter enable

2.1.11 filter dhcp

Syntax

To enable DHCP attack detection, run the following command

filter dhcp

To disable DHCP attack detection, run the no form of the previous command.

no filter dhcp

Parameter

None

Command Mode

Global configuration mode and physical port configuration mode

The command is efficient when both the global port and the physical port are configured

Example

Switch_config# filter dhcp

Switch_config# interface g0/1

switch_config_g0/1# filter dhcp

Related Commands

filter enable

2.1.12 filter arp

Syntax

To fliter ARP attack, use the filter arp command

filter arp

To resume to the default value, use the no form of the previous command

no filter arp

Parameter

None

Command Mode

Physical interface configuration

Example

Switch_config_g0/1# filter arp

Related Command

filter enable

2.1.13 filter bpdu

Syntax

To enable BPDU attack detection, run the following command

filter bpdu

To resume to the default setting, use the no form of previous command

no filter bpdu

Parameter

None

Command Mode

Physical interface configuration

Example

Switch_config_g0/1# filter bpdu

Related Commands

filter enable

2.1.14 filter mode

Syntax

To configure the filter mode, run the following command

filter mode [raw | hybrid]

Parameter

Parameter	Description
raw	To configure Filter as Raw mode
hybrid	To configure Filter as Hybrid mode

Default

Hybrid mode

Command Mode

Global configuration mode

Example

Switch_config# filter mode raw

Related Command

filter enable

2.1.15 filter enable

Syntax

To enable filter feature, use the filter enable command

filter enable

To resume to the default setting, run the no form of the previous command

no filter enable

Parameter

None

Command Mode

Global configuration mode

Example

Switch_config# filter enable

Related Command

None

2.1.16 filter shutdown-action

Syntax

To configure to shut down the port when an attack source is detected in raw mode, run the following command

filter shutdown-action

To configure not to shut down the port when an attack source is detected in raw mode,, use the no form of the previous command

no filter shutdown-action

Parameter

None

Command mode

Global configuration mode

Example

Switch_config# filter shutdown-action

Related command

None

2.1.17 show filter

Syntax

To display working state of the anti-attack feature of the current switch, use the show filter command

show filter

To resume to the default setting, use the no form of the previous command

show filter summary

Parameter

None

Command Mode

Non-user mode

Example

Switch#show filter

Filter period 600 seconds, polling interval 600 seconds

Filter thresholds:

Filter type(major code)	Minor code	Threshold	Polling
arp	A	5	3
bpdu	B	1000	750
dhcp	D	1000	750
ip	I	1000	750
icmp	I	1000	750
igmp	I	1000	750

Filters blocked:

Cause	Address	Seconds	Discard	Rate	Polling	Interface
arp	0000.abcd.1234	7.41	0	0/0	592.59	G0/1

Filters counting:

Cause	Address	Seconds	Count	Interface
arp	0000.abcd.1234	15.59	1	G0/1

Filters blocked: indicates MAC address of the blocked attack source, blocked time and source interface

Filters counting: indicates MAC address of the attack source, counting time, the number of the receiving packets and the source interface

Chapter 3 Backup Link Configuration Commands

3.1 Global Configuration Commands

3.1.1 backup-link-group *id*

Syntax

To set the BackupLink group, run the following command:

backup-link-group *id*

To delete the BackupLink group, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group, ranging from 1 to 8

Default

The backuplink group is not configured by default

Command Mode

Global configuration mode

Usage Guidelines

None

Example

Switch_config#backup-link-group 1

Switch_config#

Related Command

None

3.1.2 backup-link-group id preemption-mode forced {delay *value*}

Syntax

To set the port-based preemption mode for the backuplink group, run the following command:

backup-link-group id preemption-mode forced {delay *value***}**

To delete the port-based preemption mode for the backuplink group, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group, ranging from 1 to 8
value	Stands for the delay time, ranging from 0s to 60s

Default

The backuplink group has not been set with the trait of port-based preemption by default

Command Mode

Global configuration mode

Usage Guidelines

The **backup-link-group id preemption-mode forced {delay** value} command can be used to create the backuplink group directly

Example

Switch_config#backup-link-group 1 preemption-mode forced delay 5

Switch_config#

Related Command

backup-link-group id

backup-link-group id preemption-mode bandwidth {delay value}

3.1.3 backup-link-group id preemption-mode bandwidth {delay *value*}

Syntax

To set port bandwidth preemption mode for the backuplink group, run the following command:

backup-link-group id preemption-mode bandwidth {delay *value*}

To delete port bandwidth preemption mode for the backuplink group, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group, ranging from 1 to 8

value	Stands for the delay time, ranging from 0s to 60s

Default

The backuplink group has not been set with the trait of port bandwidth preemption by default

Command Mode

Global configuration mode

Usage Guidelines

None

Example

Switch_config#backup-link-group 1 preemption-mode bandwidth delay 5

Switch_config#

Related Command

backup-link-group id

backup-link-group id preemption-mode forced {delay value}

3.1.4 monitor-link-group id

Syntax

To set the MonitorLink group, run the following command:

monitor-link-group *id*

To delete the MonitorLink group, run the following command:

no monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group, ranging from 1 to 8

Default

The MonitorLink group is not configured by default

Command Mode

Global configuration mode

Usage Guidelines

None

Example

Switch _config# monitor-link-group 1

Switch_config#

Related Command

None

3.2 Port Configuration Commands

3.2.1 backup-link-group id active

Syntax

To set a port to be an active port, run the following command:

backup-link-group *id* **active**

To cancel the active port, run the following command:

no backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group, ranging from 1 to 8

Default

The primary port is not configured by default

Command Mode

The physical port configuration mode and the aggregation port configuration mode

Usage Guidelines

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly

Example

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#backup-link-group 1 active

Switch_config_g0/1#exit

Related Command

backup-link-group id

backup-link-group id backup

3.2.2 backup-link-group id backup

Syntax

To set a port to be a backup port, run the following command:

backup-link-group *id* **backup**

To cancel the backup port, run the following command:

no backup-link-group id

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group, ranging from 1 to 8

Default

The backup port is not configured by default

Command Mode

The physical port configuration mode and the aggregation port configuration mode

Usage Guidelines

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly

Example

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#backup-link-group 1 backup

Switch_config_g0/1#exit

Related Command

backup-link-group id

backup-link-group id active

3.2.3 share-load vlan vlanmap

Syntax

To set VLAN load balance for the backup port, run the following command:

share-load vlan *vlanmap*

To delete VLAN load balance for the backup port, run the following command:

no share-load vlan

Parameter

Parameter	Description
vlanmap	Stands for the VLAN value, ranging from 1 to 4049

Default

VLAN load balance is not set for the backup port by default

Command Mode

The physical port configuration mode and the aggregation port configuration mode

Usage Guidelines

This command can be set only on the backup port, that is, a port must be set to be a backup port before VLAN load balance is set on the port

Different BackupLink groups can be set to have the same VLAN group or the overlapped VLAN segments. If there are overlapped VLAN segments, the system will classify these VLANs into different MSTs (STGs) and conduct operations toward a group of ports, the statuses of these ports in different MSTs vary. So, you'd better rule out those overlapped VLAN groups when configuring load balance for VLANs

Example

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1# share-load vlan 100-200

Switch_config_g0/1#exit

Related Command

backup-link-group id

backup-link-group id backup

3.2.4 backup-link-group mmu transmit

Syntax

To set MMU transmission for the ports of the backuplink group, run the following command:

backup-link-group mmu transmit

To delete MMU transmission for the ports of the backuplink group, run the following command:

no backup-link-group mmu

Parameter

None

Default

The MMU transmission function for the ports of the backuplink group is not set by default

Command Mode

The physical port configuration mode and the aggregation port configuration mode

Usage Guidelines

Only the ports of the backuplink group can be set to **transmit**, that is, the ports must be set to **active** or **backup**

Example

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#backup-link-group mmu transmit

Switch_config_g0/1#exit

Related Command

backup-link-group id

3.2.5 backup-link-group mmu receive

Syntax

To set MMU reception for ports, run the following command:

backup-link-group mmu receive

To delete MMU reception for ports, run the following command:

no backup-link-group mmu

Parameter

None

Default

The MMU reception function for the ports is not set by default

Command Mode

The physical port configuration mode and the aggregation port configuration mode

Usage Guidelines

The ports that are set to **receive** are not necessarily the ports of the backuplink group

Example

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#backup-link-group mmu receive

Switch_config_g0/1#exit

Related Command

None

3.2.6 monitor-link-group id uplink

Syntax

To set a port to be an uplink port, run the following command:

monitor-link-group *id* **uplink**

To cancel the uplink port configuration, run the following command:

no monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group, ranging from 1 to 8

Default

The uplink port is not configured by default

Command Mode

The physical port configuration mode and the aggregation port configuration mode

Usage Guidelines

If the Monitorlink group is not established, it will be automatically created when you configure the Monitorlink group on a port directly

Example

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1# monitor-link-group 1 uplink

Switch_config_g0/1#exit

Related Command

monitor-link-group id

monitor-link-group id downlink

3.2.7 monitor-link-group id downlink

Syntax

To set a port to be a downlink port, run the following command:

monitor-link-group *id* **downlink**

To cancel the downlink port configuration, run the following command:

no monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group, ranging from 1 to 8

Default

The downlink port is not configured by default

Command Mode

The physical port configuration mode and the aggregation port configuration mode

Usage Guidelines

If the Monitorlink group is not established, it will be automatically created when you configure the Monitorlink group on a port directly

Example

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1# monitor-link-group 1 downlink

Switch_config_g0/1#exit

Related Command

monitor-link-group id

monitor-link-group id uplink

3.3 how Configuration Commands

3.3.1 show backup-link-group id

Syntax

To display the information about the backuplink group, run the following command:

show backup-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the backuplink group, ranging from 1 to 8

Default

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

Switch_config# show backup-link-group 1

Active Interface Backup Interface State Vlan State

GigaEthernet0/2 GigaEthernet0/4 Forward/Block Block/Block

Share load vlan: 100-200,port[GigaEthernet0/4] vlan state: Forwarding

Preemption Mode: No Preempt

Preemption Delay: 0 seconds

Related Command

None

3.3.2 show monitor-link-group id

Syntax

To display the information about the monitorlink group, run the following command:

show monitor-link-group *id*

Parameter

Parameter	Description
Id	Stands for the instance ID of the monitorlink group, ranging from 1 to 8

Default

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

```
Switch_config#show monitor-link-group 1
uplink interface: GigaEthernet0/2        Forwarding
downlink interface:
GigaEthernet0/1        Forwarding
GigaEthernet0/3        Forwarding
```

Related Command

None

Chapter 4 System Management Commands

4.1 File Management Configuration Commands

4.1.1 copy

Syntax

To read a file from the tftp server to a switch, use the **copy** command

copy tftp<:*filename*> {**flash**<:*filename*>|**rom**} [*ip_addr*]

Parameter

Parameter	Description
tftp<:filename>	Read a file from the tftp server. Filename indicates the relevant filename. If not specified the filename, the system will prompt user to input the filename after executing the copy command
flash <:filename>	Write a file to the flash memory of the switch. Filename indicates the relevant filename. If not specified the filename, the system will prompt user to input the filename after executing the copy command
rom	Updates bootrom for the switch
ip_addr	Specifies the IP address of tftp srever. If not specified, the system will prompt user to input the IP address after executing the copy command

Default

None

Command Mode

Monitor mode

Usage Guidelines

None

Example

monitor#copy tftp:switch.bin flash:switch.bin 192.2.2.1

The example shows how to read the switch.bin from the tftp server to the flash memory of the switch:

Related Command

None

4.1.2 delete

Syntax

To delete a file, use the **delete** command

delete *file-name*

Parameter

Parameter	Description
file-name	Specifies the filename (maximum 20 characters)

Default

If not specified the file-name, the system will delete startup-config by default

Command Mode

Monitor mode

Usage Guidelines

None

Related Command

None

4.1.3 dir

Syntax

To display filename, use the **dir** command

dir *file-name*

Parameter

Parameter	Description
file-name	Specifies the filename (maximum 20 characters)

Default

None

Command Mode

monitor mode

Usage Guidelines

None

Related Command

None

4.1.4 ip address

Syntax

To set an IP address for an Ethernet interface, use the **ip address** command

ip address *ip-address mask*

Parameter

Parameter	Description
ip-address	IP address
mask	IP network mask

Default

None

Command Mode

Monitor mode

Usage Guidelines

None

Example

monitor#ip address 192.168.1.1 255.255.255.0

Related Command

ip route

ping

4.1.5 ip route

Syntax

To set the default gateway, run the following command:

ip route default gw_ip_addr

Parameter

Parameter	Description
gw_ip_addr	The address of the default gateway

Default

None

Command Mode

The monitoring state

Usage Guidelines

None

Example

monitor#ip default-gateway 192.168.1.3

Related Command

ip address

4.1.6 show configuration

Syntax

To display the running configuration file, use the **show configuration** command

show configuration

Parameter

None

Default

None

Command Mode

Monitor mode

Usage Guidelines

None

Related Command

None

4.1.7 format

Syntax

To format file system, use the **format** command

format

Parameter

None

Default

None

Command Mode

EXEC

Usage Guidelines

All files in the file system will de deleted after executing the **format** command

Related Command

None

4.1.8 more

Syntax

To display the contents of a file, use the more command

more file-name

Parameter

Parameter	Description
file-name	Specifies the name of a file (maximum 20 characters)

Default

None

Command Mode

EXEC

Usage Guidelines

If all files are displayable characters, they will be displayed in ASCII format, or they will be displayed binary format

Related Command

None

4.2 Basic System Management Commands

4.2.1 boot flash

Syntax

To enable the system from the specified file in monitor mode, use the boot flash command

boot flash filename

Parameter

Parameter	Description
filename	Specified file name

Default

None

Command Mode

Monitor mode

Usage Guidelines

Use the boot flash command to enable the device after user entering the monitor mode

Example

monitor#boot flash switch.bin

Related Command

None

4.2.2 cd

Syntax

To change the current directory, use the **cd** command

cd *directory*|..

Parameter:

Parameter	Description
directory	Name of the directory. (maximum 20 characters)
..	Upper directory

Default

None

Command Mode

Monitor mode

Usage Guidelines

None

Example

monitor#cd my_dir

Related Command

pwd

4.2.3 chinese

Syntax

To switch command prompt to chinese mode, use the **chinese** command

Parameter

None

Default

None

Command Mode

Monitor mode

Usage Guidelines

None

Example

None

Related Command

None

4.2.4 date

Syntax

To set the absolute time, use the date command

Parameter

None

Default

None

Command Mode

Monitor mode

Usage Guidelines

This command is used to set the abslute time for the system. For the switch with a battery-powered clock, the clock will be powered by the battery. If the clock doesn't keep good time, you need to change the battery

For the swich without a battery-powered clock, the system date is configured to July 1st, 1970 after the reboot of the switch, and user needs to set the current time each time when starting the switch

Example

monitor#date

The current date is 2000-7-27 21:17:24

Enter the new date(yyyy-mm-dd):2000-7-27

Enter the new time(hh:mm:ss):21:17:00

Related Command

4.2.5 english

Syntax

To switch the command prompt to english mode, use the **english** command

Parameter

None

Default

None

Command Mode

Monitor mode

Usage Guidelines

None

Example

None

Related Command

None

4.2.6 md

Syntax

md directory

Parameter

Parameter	Description
directory	Name of directory (maximum 20 characters)

Default

None

Command Mode

Monitor mode

Usage Guidelines

To set a directory, use the **md** command

Related Command

None

4.2.7 pwd

Parameter

None

Default

None

Command Mode

Monitor mode

Usage Guidelines

To display the current directory, use the **pwd** command

Related Command

None

4.2.8 rd

Syntax

rd directory

Parameter

Parameter	Description
directory	Name of the directory(maximum 20 characters)

Default

None

Command Mode

Monitor mode

Usage Guidelines

The system prompts if the directory is not empty. The system prompts if the directory doesn't exist. To delete a command, use the rd command

Related Command

None

4.2.9 rename

Syntax

To rename a file in a file system, use the **rename** command

rename *old_file_name* *new_file_name*

Parameter

Parameter	Description
old_file_name	The original filename
new_file_name	The new filename

Default

None

Command Mode

Monitor mode

Usage Guidelines

None

Related Command

None

4.2.10 reboot

Parameter

None

Default

None

Command Mode

Monitor mode

Usage Guidelines

To reboot a switch, use the **reboot** command

Related Command

None

4.2.11 alias

Syntax

alias *alias_name command_line*

Parameter

Parameter	Description
alias_name	Name the alias name
command_line	The command of naming the alias name

Default

None

Comand mode

Global configuration mode

Usage Guidelines

The command can be used to replace "command_line" with "alias_name". For instance, alias update1 copy tftp: switch.bin flash:switch.bin 10.168.30.188. The command " copy tftp: switch.bin flash:switch.bin 10.168.30.188 " will automatically run on the OLT only update 1 is input

Example

The following example shows how to use the command to replace " copy tftp:BDMSU8508_4.0.0B.bin flash:switch.bin 10.168.30.188" with " update1"

alias update1 copy tftp:BDMSU8508_4.0.0B.bin flash:switch.bin 10.168.30.188

Related Command

None

4.2.12 boot system flash

Syntax

Run the **boot system flash** command to specify the systematic mirroring files when the system is started up. Run the no **boot system flash** command to delete the previous configuration

boot system flash *filename*

no boot system flash *filename*

Parameter

Parameter	Description
filename	It is the specified filename, which contains no more than 20 characters

Default

None

Command Mode

Global configuration mode

Usage Guidelines

If you have not configured the command, the system will execute the first systematic mirroring file in the flash file system. If you have configured multiple commands, the system will execute the mirroring files one by one. If the file does not exist or the check sum is wrong, the system will execute the next file. If both fail, the system will run at the monitoring state

Example

config#boot system flash switch.bin

Related Command

None

4.2.13 help

Syntax

help

Parameter

None

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to display the help system of the switch

Example

The foloowing example shows how to display the help system of the switch, after you enter the command

switch# help

Help may be requested at any point in a command by entering a question mark '?', If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options

Two styles of help are provided:

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

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

Related Command

None

4.2.14 history

Syntax

The command is used to check the historical commands. Run the **[no] history** command to delete the historical commands

[no] history [+ <*count*> | - <*count*> | clear]

Parameter

Parameter	Description
+ <count>	Displays the count<1-20> historical command from the beginning to the end
- <count>	Displays the count<1-20> historical command from the end to the beginning

Default

If there are no more than 20 commands executed, all historical command lines will be displayed from the beginning to the end. If there are more than 20 commands executed, the latest 20 command lines will be displayed from the beginning to the end

Command Mode

Abandom command mode

Usage Guidelines

The modularized switch can save up to 20 historical commands. You can invoke these commands with the "up" or "down" key or directly use it after edition

Example

The following example shows the latest five commands from the end to the beginning:

switch#history - 5

config

int e1/1

no ip addr

ip addr 192.2.2.49 255.255.255.0

exit

Related Command

None

4.2.15 show

Syntax

To display the relevant information of the system, which or specific ones of which can be filtered through the filter, run the following command:

show <sub-command> [| <begin | include | exclude | redirect> <*WORD*> [*SEPARATOR WORD*]]

Parameter

Parameter	Description
sub-command	Stands for a child command
|	Uses the output filter
begin	Means to show the result of the **show** command starting with a specific word
include	Means to show the sentences of the result of the **show** command containing a specific word
exclude	Means not to show the lines of the result of the **show** command containing a specific word
redirect	Redirects the result of the **show** command to the file in the designated file system
WORD	Stands for a designated word, which is the designated filename as to the **redirect** command
SEPARATOR WORD	Stands for the designated separator, which is space by default to separate the words

Default

None

Command Mode

EXEC mode or global configuration mode

Usage Guidelines

This command can be used to filter the useless information in the result of the show command, especially when the result is too much to read. For example, if you want to browse a designated MAC address in an MAC address table, which contains a lot of MAC addresses, this command will give you convenience for you

Example

The following example shows how to display the lines, in which the word "interface" is contained, in the result of **show running-config**

```
Switch#show running-config | include interface
Building configuration...


Current configuration:
!
interface GigaEthernet0/1
interface GigaEthernet0/2
interface GigaEthernet0/3
interface GigaEthernet0/4
interface GigaEthernet0/5
interface GigaEthernet0/6
interface GigaEthernet0/7
interface GigaEthernet0/8
```

Related Command

None

4.2.16 show alias

Syntax

To display all alias commands, or the alias commands in a specified mode, use the show aliases command.
show alias [<*alias name*>]

Parameter

parameter	description
alias name	Alias command

Default

Display all alias commands in the format of alias name=command line

Command Mode

EXEC mode or global configuration mode

Usage Guidelines

None

Example

The following example shows how to use the command to display all alias names:
switch_config#show alias
hualab=date
router=snmp

Related Command

alias

4.2.17 show break

Syntax

It is used to display the abnormal information of the system. The system stores all abnormal information in the latest running. The abnormal information contains the times of abnormity, the stack content and the invoked functions when abnormity occurs

Parameter

None

Default

None

Command Mode

Monitor mode

Usage Guidelines

The command is only used for debugging

Related Command

None

Chapter 5 Terminal Service Configuration Commands

5.1 Telnet Configuration Commands

5.1.1 telnet

Syntax

The following is a command for establishing a telnet session:
telnet *server-ip-addr/server-host-name* [**/port** *port*][**/source-interface** *interface*] [**/local** *local-ip-addr*] [**/debug**][**echo/noecho**] [**/script** *scriptname*]

Parameter

Parameter	Description
server-ip-addr	Dotted-decimal IP address of the remote server
server-host-name	Name of the remote server, which is configured by the **ip host** command
port	Telnet port of the remote server
interface	Local interface where the telnet connection is originated
local-ip-addr	Local IP address where the telnet connection is originated
/debug	A negotiation process for openning the debug at the client side and printing the connection
/echo */noecho*	Enable or disable the local echo. The default value is **noecho**
scriptname	A script name used for auto login

Default

The default port number is 23. The interface has no default number

Command Mode

EXEC mode or global configuration mode

Usage Guidelines

You can use one of the following command lines to establish a remote login.
telnet server-ip-addr/server-host-name
In this case, the application program directly sends the telnet login request to port 23 of the remote server. The local IP address is the IP address which is nearest to the peer and found by the routing table.
telnet server-ip-addr/server-host-name /port port
In this case, the application program sends a telnet login request to the port of the peer.
telnet server-ip-addr/server-host-name /source-interface interface

In this case, the application program uses the IP address on the interface ass the local IP address.

telnet server-ip-addr/server-host-name /debug

In this case, the application program opens the debug and exports the connection at the client side.

telnet server-ip-addr/server-host-name echo/noecho

In this case, the application program enables or disables the local echo. The local echo is disabled by default. The echo is completed at the server side. Only when the server is not in charge of echo is the local echo enabled.

telnet server-ip-addr/server-host-name /script scriptname

Before executing the automatic login command of the script, run the command **ip telnet script** to configure the script.

The previous commands can be used together.

During the session with the remote server, you can press the **Q** button to exit the session. If the session is not manually closed, the session will be complete after a 10-second timeout.

Example

Suppose you want to telnet server 192.168.20.124, the telnet port of the server is port 23 and port 2323, and the local two interfaces are e1/1(192.168.20.240) and s1/0(202.96.124.240). You can run the following operations to complete the remote login.

1.telnet 192.168.20.124 /port 2323

In this case, the telnet connection with port 2323 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

2.telnet 192.168.20.124 /source-interface s1/0

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 202.96.124.240.

3. telnet 192.168.20.124 /local 192.168.20.240

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

4. telnet 192.168.20.124 /debug

In this case, the telnet connection negotiation with port 23 of the peer will be printed out.

5. telnet 192.168.20.124 /echo

In this case, the local echo is enabled. If the echo is also enabled at the server side, all input will be echoed twice.

6. telnet 192.168.20.124 /script s1

Use login script S1 for automatic login.

5.1.2 ip telnet

Syntax

The following are the configuration commands of the telnet session:

ip telnet source-interface vlan *value*

ip telnet access-class *accesslist*

ip telnet listen-port *start-port [end-port]*

ip telnet script *scriptname 'user_prompt' user_answer 'pwd_prompt' pwd_answer*

Parameter

Parameter	Description
num	Maximum number of Telnet connections.
value	Local interface where the telnet request is originated
accesslist	Access list name to limit the source address when the local client receives the connection
start-port	Starting port number designated at the listening port area

end-port	End port number designated at the listening port area
scriptname	Name of the login script
user_prompt	Username prompt returned by the telnet server
user_answer	Username response information from the client side
pwd_prompt	Password prompt returned by the telnet server
pwd_answer	Password response information submitted by the client side

Default

None

Command Mode

Global configuration

Usage Guidelines

• Run the following command to configure the local interface for originating the telnet connection:

ip telnet source-interface *interface*

In this case, all telnet connections originated afterwards are through the interface. The configuration command is similar to the command **telnet source-interface *interface***. However, the **telnet** command has no interface parameters followed. When the interface is configured and the **telnet** command has interface parameters, the interface followed the telnet command is used

• Run the following command to configure the name of the access list which performs limitation on local telnet connection reception

ip telnet access-class *accesslist*

In this case, the access list will be checked when the server accepts all telnet connections

• Run the following command to configure a port, except the default port 23, to receive the telnet service

ip telnet listen-port *start-port [end-port]*

Usage Guidelines: If the end port number is not designated, the listening will be executed at a specific port. The number of the designated ports cannot be bigger than 16 and the port number ranges between 3001 and 3999

• Run the following command to configure the telnet login script

ip telnet script s1 'login:' switch 'Password:' test

Usage Guidelines: When the script is configured, the username prompt and password prompt and their answers must be correctly matched, especially the prompt information is capital sensitive and has inverted comma (''). If one of them is wrongly configured, the automatic login cannot be performed

Note:

You can add the NO prefix on the above four commands and then run them to cancel previous configuration.

Example

1.ip telnet source-interface vlan1
In this case, the interface vlan1 will be adopted to originate all telnet connections afterwards
2. ip telnet access-class abc
In this case, all the received telnet connections use access list **abc** to perform the access list check
3. ip telnet listen-port 3001 3010
Except port 23, all ports from port 3001 to port 3010 can receive the telnet connection.

4. ip telnet script s1 'login:' switch 'Password:' test
The login script **s1** is configured. The username prompt is **login:** and the answer is **switch**. The password prompt is **Password:** and the answer is **test**

5.1.3 ctrl-shift-6+x (the current connection is mounted)

Syntax

Run the following command to mount the current telnet connection:
ctrl-shift-6+x

Parameter

None

Default

None

Command Mode

Any moment in the current telnet session

Usage Guidelines

You can use the shortcut key to mount the current telnet connection at the client side

Example

switchA>telnet 192.168.20.1
Welcome to Multi-Protocol 2000 Series switch
switchB>ena
switchB#(press ctrl-shift-6+x)
switchA>
You press **ctrl-shift-6+x** to mount the telnet connection to switch B and return to the current state of switch A

5.1.4 where

Syntax

Run the following command to check the currently mounted telnet session:
where

Parameter

None

Default

None

Command Mode

Global configuration

Usage Guidelines

You can use the command to check the mounted outward telnet connection at the client side. The displayed information contains the serial number, peer address, local address and local port.

Note:

The **where** command is different from the **show telnet** command. The former is used at the client side and the displayed information is the outward telnet connection. The latter is used at the server and the displayed information is the inward telnet connection

Example

switchA>telnet 192.168.20.1

Welcome to Multi-Protocol 2000 Series switch

switchB>ena

switchB#(Press ctrl-shift-6+x)

switchA> telnet 192.168.20.2

Welcome to Multi-Protocol 2000 Series switch

switchC>ena

switchC#(Press ctrl-shift-6+x)

switchA>where

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.1	23	192.168.20.180	20034
2	192.168.20.2	23	192.168.20.180	20035

Enter **where** at switch A. The mounted outward connection is displayed

5.1.5 resume

Syntax

The following command is used to resume the currently mounted outward telnet connection:
resume *no*

Parameter

Parameter	Description
no	Number of the currently mounted telnet session that is checked through the **where** command

Default

None

Command Mode

Global configuration

Usage Guidelines

The command can be used to resume the currently mounted outward telnet connection at the client side

Example

switchA>telnet 192.168.20.1

Welcome to Multi-Protocol 2000 Series switch

switchB>ena

switchB#(press ctrl-shift-6+x)

switchA> telnet 192.168.20.2

Welcome to Multi-Protocol 2000 Series switch

switchC>ena

switchC#(press ctrl-shift-6+x)

switchA>where

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.1	23	192.168.20.180	20034
2	192.168.20.2	23	192.168.20.180	20035

switchA>Resume 1

[Resuming connection 1 to 192.168.20.73 . . .]

(enter)

switchB#

After you enter **where** at switch A and the mounted outward connection of switch A is displayed. When entering **Resume1**, you will be prompted that connection 1 is resumed. The command prompts of switch B are displayed after the **Enter** key is pressed

5.1.6 disconnect

Syntax

The following command is used to clear the currently mounted outward telnet session:
disconnect *no*

Parameter

Parameter	Description
No	Number of the currently mounted telnet session that is checked through the **where** command

Default

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to clear the currently mounted outward telnet connection at the client side
Note:

The **disconnect** command is different from the **clear telnet** command. The former is used at the client side and clears the outward telnet connection. The latter is used at the server and clears the inward telnet connection

Example

switchA>telnet 192.168.20.1

Welcome to Multi-Protocol 2000 Series switch

switchB>ena

switchB#(press ctrl-shift-6+x)

switchA> telnet 192.168.20.2

Welcome to Multi-Protocol 2000 Series switch

switchC>ena

switchC#(press ctrl-shift-6+x)

switchA>where

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.1	23	192.168.20.180	20034
2	192.168.20.2	23	192.168.20.180	20035

switchA>disconnect 1

<Closing connection to 192.168.20.1> <y/n>y

Connection closed by remote host.

switchA>

After you enter **where** at switch A and the mounted outward connection of switch A is displayed, enter **disconnect 1**. You will be prompted whether the connection of switch B is closed. After you enter **Y**, the connection is closed

5.1.7 clear telnet

Syntax

The following is a command format to clear the telnet session at the server:
clear telnet *no*

Parameter

Parameter	Description
no	Number of the telnet session that is displayed after the **show telnet** command is run

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to clear the telnet session at the server

Example

clear telnet 1
The telnet session whose sequence number is 1 is cleared at the server

5.1.8 show telnet

Syntax

The following is a command format to display the telnet session at the server:

show telnet

Parameter

None

Default

None

Command Mode

All command modes except the user mode

Usage Guidelines

The command is used to display the telnet session at the server. The displayed information includes the sequence number, peer address, peer port, local address and local port.

Example

Switch# show telnet

If you run the previous command, the result is shown as follows:

NO.	Remote Addr	Remote Port	Local Addr	Local Port
1	192.168.20.220	1097	192.168.20.240	23
2	192.168.20.180	14034	192.168.20.240	23

5.1.9 debug telnet

Syntax

The following is a format of the **debug** command for the telnet session:

debug telnet

Parameter

None

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable the telnet debug
If the switch of the telnet debug is opened, the negotiation processes of all the incoming telnet sessions are printed on the window that the debug command invokes. The **debug telnet** command is different from the **telnet debug** command. The former is to export the debug information of the telnet session connected to the server. The latter is to export the debug information of the telnet session that the client originates

Example

debug telnet

After using the comamnd, the debug information of the telnet session that is connected to the server is displayed

5.2 Terminal Configuration Commands

5.2.1 attach-port

Syntax

The following command is to bind the telnet listening port to the **line vty** number and enable the telnet connection at a specific port generates **vty** according to the designated sequence number
[no] attach-port *PORT*

Parameter

Parameter	Description
port	Listening port of the telnet server (3001-3999)

Default

None

Command Mode

Line configuration mode

Example

The following example shows how to bind listening port 3001 to line vty 2 3
switch_config# line vty 2 3
switch_config_line#attach-port 3001

5.2.2 autocommand

Syntax

It is used to set the automatically-run command when user logs in to the terminal. The connection is cut off after the command is executed
autocommand *LINE*

no autocommand

Parameter

Parameter	Description
LINE	Command to be executed

Command Mode

Line configuration mode

Example

switch_conf#line vty 1
switch_conf_line#autocommand pad 123456
After you successfully log in, the host whose X.121 address is 123456 will be automatically padded.

5.2.3 clear line

Syntax

To clear the designated line, use the following command:
clear line [*aux* | *tty* | *vty*] [*number*]

Parameter

Similar to the **line** command

Command Mode

EXEC mode

Example

switch#clear line vty 0

5.2.4 connect

Syntax

To connect the telnet server, use the following command:
connect *server-ip-addr/ server-host-name* {[/**port** *port*][/**source-interface** *interface*] [/**local** *local-ip-addr*]} [/**script** *word*]

Parameter

Parameter	Description
server-ip-addr/server-host-name	IP address of the server or the host name of the server
port	Port number
interface	Name of the interface where the connection is originated
local-ip-addr	Local IP address where the connection is originated
word	Name of the script

Command Mode

All configuration modes

Example

switch# connect 192.168.20.1

5.2.5 disconnect

Syntax

To delete the mounted telnet session, use the following command:

disconnect *N*

Parameter

Parameter	Description
N	Number of the mounted telnet session

Command Mode

All configuration modes

Example

switch#disconnect 1

5.2.6 exec-timeout

Syntax

To set the maximum spare time for the terminal, use the following command:
[**no**] **exec-timeout** [*time*]

Parameter

Parameter	Description
time	Spare time whose unit is second.. Range: 0-864000.

Default

0 (No time-out limitation)

Command Mode

Line configuration mode

Example

Set the spare time of the line to one hour.
switch_config_line#exec-timeout 3600

5.2.7 length

Syntax

To set the line number on the screen of the terminal, use the following command:

[**no**] **length** [*value*]

Parameter

Parameter	Description
value	A value between 0 and 512 The value **0** means there is no pause

Default

24

Command Mode

Line configuration mode

5.2.8 line

Syntax

To enter the line configuration mode, use the following command:
line [**aux | console | tty | vty**] [*number*]

Parameter

Parameter	Description
console	Monitoring line, which has only one number **0**
vty	Virtual lines such as Telnet, PAD and Rlogin
number	Number in the line of the type

Command Mode

Global configuration mode

Example

The following example shows how to enter the line configuration mode of VTY 0 to 10
switch_config#line vty 0 10

5.2.9 location

Syntax

To recoded the description of the current line, use the following command. To return to the default setting, use the no form of this command
location [*LINE*]

no location

Parameter

Parameter	Description
LINE	Description of the current line

Command Mode

Line configuration mode

5.2.10 login authentication

Syntax

To set line login authentication parameters, use the following command. To return to the default setting, use the no form of this command
[**no**] **line login authentication** [**default** / *WORD*]

Parameter

Parameter	Description
Default	Default authentication mode
WORD	Name of the authentication list

Command Mode

Line configuration mode

Example

switch_conf_line#login authentication test
In the example, the authentication list of the line is set to **test**

5.2.11 monitor

Syntax

To export the log and debugging information to the line, use the following command. To return to the default setting, use the no form of this command

[**no**] **monitor**

Parameter

None

Command Mode

Line configuration mode

Example

switch_config_line#monitor

5.2.12 no debug all

Syntax

To shut down all debugging output of the current VTY, use the following command.

no debug all

Parameter

None

Command Mode

EXEC mode

Example

switch#no debug all

5.2.13 password

Syntax

To set the password for the terminal, use the following command. To return to the default setting, use the no form of this command.

password {*password*| [encryption-type] *encrypted-password*}

no password

Parameter

Parameter	Description
password	Password configured on the line, which is entered in the plaintext form and whose maximum length is 30 bits
[encryption-type] encrypted-password	**encryption-type** means the encryption type of the password Currently, MY COMPANY products only support two encryption modes: 0 and 7. The number **0** means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm defined by MY COMPANY. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches

For password encryption, refer to the explanation of the commands **service *password-encryption*** and **enable password**

Command Mode

Line configuration mode

Example

switch_conf#line vty 1
switch_conf_line#password test
The previous example shows the login password of VTY1 is set to **test**

5.2.14 resume

Syntax

To resume the mounted telnet session, use the following command.

resume *N*

Parameter

Parameter	Description
N	Number of the mounted telnet session

Command Mode

All configuration modes

Example

switch#resume 1

5.2.15 show debug

Syntax

To display all debugging information of the current VTY, use the following command

show debug

Parameter

None

Command Mode

EXEC mode or global configuration mode

Example

Switch# show debug
http authentication debug is on
http cli debug is on

http request debug is on
http response debug is on
http session debug is on
http erro debug is on
http file debug is on
TELNET:
Incoming Telnet debugging is on

5.2.16 show line

Syntax

To display the status of the current effective line, use the following command
show line {[**console** | **vty**] [*number*]}}

Parameter

If there is no parameter followed, the status of all effective lines will be displayed

The definition of other parameters is similar to that of the **line** command

Command Mode

All configuration modes except the user mode

5.2.17 terminal length

Syntax

It is used to change the line number on the current terminal screen. The parameter can be obtained by the remote host. The rlogin protocol uses the parameter to notify the remote UNIX host. Run the **no terminal length** command to resume the default value:
terminal length *length*

no terminal length

Parameter

Parameter	Description
Length	Line number displayed on each screen Range: 0-512

Default

Pause when 24 lines are displayed on the screen

Command Mode

Global configuration mode

Usage Guidelines

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid

Example

switch#terminal length 40

Related Command

line

5.2.18 terminal monitor

Syntax

It is used to display the debugging output information and system faulty information at the current terminal. The no form of the command is used to disable the monitoring:

terminal monitor

no terminal monitor

Parameter

None

Default

The system monitoring port (console) is open by default. Other terminals are closed by default

Command Mode

Global configuration

Usage Guidelines

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid

Example

switch#terminal monitor

Related Command

line

debug

5.2.19 terminal width

Syntax

In default settings, the switch is to export 80 characters in each line. If the default settings cannot meet your requirements, you can reset it. The parameter can be obtained by the remote host. Run the **terminal width** command to set the character number in each line. Run the **no terminal width** command to resume to the default value

terminal width *number*

no terminal width

Parameter

Parameter	Description
number	Character number of each line

Default

Display 80 characters in each line

Command Mode

Global configuration

Usage Guidelines

The command is effective only to the current terminal. When the session is complete, the terminal attribute is invalid

Example

switch#terminal width 40

Related Command

line

5.2.20 terminal-type

Syntax

To set the terminal type, use the following command
[**no**] **terminal-type** [*name*]

Parameter

Parameter	Description
Name	Terminal name Terminal types currently supported are VT100, ANSI and VT100J

Default

ANSI

Command Mode

Line configuration mode

5.2.21 where

Syntax

To check the currently mounted outward telnet session at the client side, use the following command

where

Parameter

None

Command Mode

All configuration modes

Example

switch#where

5.2.22 width

Syntax

To set the terminal width of the line, use the following command. To return to the default setting, use the no form of this command
[**no**] **width** [*value*]

Parameter

Parameter	Description
Value	A value between 0 and 256 The value 0 means no execution

Default

80

Command Mode

Line configuration mode

Chapter 6 Maintenance and Debugging Tool Commands

6.1 Network Testing Tool Commands

6.1.1 ping

Syntax

It is used to test host accessibility and network connectivity. After the **ping** command is run, an ICMP request message is sent to the destination host, and then the destination host returns an ICMP response message.
ping [-a][-d][**-f**] [**-i** {source-ip-address}] [-**m** {source-interface}] [**-j** host1 [host2 host3 …]] [**–k** host1 [host2, host3 …]] [**-l** length] [**-n** number] [**-r** hops] [**-s** tos] [**-t** ttl] [**-v**] [**-w** *waittime*] [–**b** *interval*] [-**c**] **host**

Parameter

Parameter	Description
-a	Sets ping all along until it is been interrupted
-d	Sets not apply the routing table
-f	Sets the DF digit (message is not segmented) If the message required to be sent is larger than the MTU of the path, the message will be dropped by the routing switch on the path and the routing switch will then return an ICMP error message to the source host. If network performance has problems, one node in the network may be configured to a small MTU. You can use the –**f** option to decide the smallest MTU on the path Default: No resetting
-i	Sets the source IP address of the message or the IP address of an interface Default: Main IP address of the message-sending interface
source-ip-address	Source IP address adopted by the message
source-interface	Message takes the IP address of the **source-interface** interface as the source address
-**j** host1 [host2 host3…]	Sets the relaxation source route Default: Not set
-**k** host1 [host2 host3…]	Sets the strict source route Default: Not set
-**l** length	Sets the length of ICMP data in the message. Default: 56 bytes
-**n** number	Sets the total number of messages. Default: 5 messages
-**r** hops	Records routes

	Up to **hops** routes are recorded Default: not record
-**s** tos	Sets IP TOS of the message to **tos** Default: 0
-**t** ttl	Sets IP TTL of the message to **ttl** Default: 255
-**v**	Detailed output
-**w** waittime	Time for each message to wait for response Default: 2 seconds
-**b** interval	Sets the time interval of sending ping packet Unit: 10ms; Value range: 0-65535; Default Value: 0
-**c**	Simple output
host	Destination host

Command Mode

EXEC mode, global configuration mode

Usage Guidelines

The command supports that the destination address is the broadcast address or the multicast address. If the destination address is the broadcast address (255.255.255.255) or the multicast address, the ICMP request message is sent on all interfaces that support broadcast or multicast. The routing switch is to export the addresses of all response hosts. By pinging multicast address 224.0.0.1, you can obtain the information about all hosts in directly-connected network segment that support multicast transmission
Press the **Q** or **q** key to stop the **ping** command
Simple output is adopted by default

Parameter	Description
!	A response message is received
.	Response message is not received in the timeout time
U	The message that the ICMP destination cannot be reached is received
Q	The ICMP source control message is received
R	The ICMP redirection message is received
T	The ICMP timeout message is received
P	The ICMP parameter problem message is received

The statistics information is exported:

Parameter	Description
packets transmitted	Number of transmitted messages
packets received	Number of received response messages, excluding other ICMP messages
packet loss	Rate of messages that are not responded to
round-trip min/avg/max	Minimum/average/maximum time of a round trip (ms)

Example

```
switch#ping -l 10000 -n 30 192.168.20.125
PING 192.168.20.125 (192.168.20.125): 10000 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 192.168.20.125 ping statistics ---
30 packets transmitted, 30 packets received, 0% packet loss
round-trip min/avg/max = 50/64/110 ms
```

6.1.2 traceroute

Syntax

It is used to detect which routes have already reached the destination
You can transmit to the destination the UDP packets (or ICMP ECHO packets) of different TTLs to confirm which routes have come to the destination. Each router on this path has to deduct 1 from the TTL value before forwarding ICMP ECHO packets. Speaking from this aspect, TTL is an effective hop count. When the TTL value of a packet is deducted to zero, the router sends back to the source system the ICMP timeout message.
By checking the ICMP timetout message sent back by intermedial routers, you can confirm the routers. At the arrival of the destination, the traceroute sends a UPD packet whose port ID is larger than 30000; the destination node hence can only transmit back a Port Unreachable ICMP message. This reception of this message means the arrival of destination
traceroute [**-i** source-ip-address] [**-m** source-interface}] [**-j** host1 [host2 host3 …]] [**–k** host1 [host2, host3 …]] [**-p** port-number] [**-q** probe-count] [**-r** hops] [**-t** ttl] [**-w** *waittime*] [**-x icmp**] **host**

Parameter

Parameter	Description
-i source-ip-address	Sets the source IP address of packet
-m source-interface	Sets the packet-transmitted port
-j host1 [host2 host3…]	Sets the loose source route. Default: Not set
-k host1 [host2 host3…]	Sets the strict source route. Default: Not set

-**p** port-number	Sets the ID of destination port that transmits UDP packets. Default: 33434
-**q** probe-count	Sets the number of packets that you detect each time Default: 3 packets
-**r** hops	Records the routes (at most hops routes can be recorded) Default: The routes are not recorded
-**t** ttl	Sets the IP TTL of packets as TTL. Default: the minimum and maximum TTLs are 1 and 30 respectively
-**w** waittime	Means the time that each packet waits for echo Default: 3 seconds
-**x icmp**	Sets the detection packet to be the ICMP ECHO packet Default: UDP packet
host	Means the destination host

Command Mode

EXEC or global configuration mode

Usage Guidelines

The UDP packet is used for detection by default, but you can run **–x icmp** to replace it with ICMP ECHO for detection
If you want to stop traceroute, press **q** or **Q**
By default, the simple output information is as follows

Parameter	Description
!N	Receives an ICMP-route unreachable packet
!H	Receives an ICMP-host unreachable packet
!P	Receives an ICMP-protocol unreachable packet
!F	Receives an ICMP unreachable (need to be fragmented) packet
!S	Receive an ICMP unreachable (failing to detect the source-station route) packet

The exported statistics information is as follows:

Parameter	Description
hops max	Means the maximum detection hops (the threshold of ICMP)

byte packets	Stands for the size of each detection packet

Example

```
switch#traceroute 90.1.1.10
traceroute to 90.1.1.10 (90.1.1.10), 30 hops max, 36 byte packets
 1    90.2.2.1    0 ms    0 ms    0 ms
      2    90.1.1.10    0 ms    0 ms    0 ms
```

6.2 Fault Diagnosis Commands

6.2.1 logging

Syntax

To record the log information to the **syslog** server, use the following command. To return to the default setting, use the no form of this command
logging *A.B.C.D*
no logging *A.B.C.D*

Parameter

Parameter	Description
A.B.C.D	IP address of the **syslog** server
level	Level of log information on the server Refer to table 1

Default:

The log information is not recorded to the server

Command Mode

Global configuration mode

Usage Guidelines

The **logging** command is used to record the log information to the designated **syslog** server. It can be used for many times to designate multiple **syslog** servers

Example

logging 192.168.1.1 errors

Related Command

logging trap

6.2.2 logging buffered

Syntax

To record the log information to the memory of the switch, use the following command. To return to the default setting, use the no form of this command.
logging buffered [*size* | *level* | *dump*]

no logging buffered

Parameter

Parameter	Description
size	Size of memory cache Value range: 4096-2147483647 Unit: byte
level	Information level of the log recorded to memory cache Refer to table 1
dump	When the system has abnormality, the information in the current memory is currently recorded to the flash and the information is resumed after the system is restarted

Default

The information is not recorded to the memory cache

Command Mode

Global configuration mode

Usage Guidelines

The command records the log information to the memory cache of the switch. The memory cache is circularly used. After the memory cache is fully occupied, the latter information will cover the previous information.
You can use the **show logging** command to display the log information recorded in the memory cache of the switch.
Do not use big memory for it causes the shortage of memory

Table 1 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR

warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Related Command

clear logging
show loggin

6.2.3 logging console

Syntax

Run the command **logging console** to control the information volume displayed on the console.
Run the command **no logging console** to forbid the log information to be displayed on the console:
logging console */level*
no logging console

Parameter

Parameter	Description
/level	Information level of the logs displayed on the console Refer to table 2

Default

The log level displayed on the console port is debugging by default

Command Mode

Global configuration mode

Usage Guidelines

After the information level is specified, information of this level or the lower level will be displayed on the console
Run the command **show logging** to display the currently configured level and the statistics information recorded in the log

Table 2 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT

critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging console alerts

Related Command

logging facility

show logging

6.2.4 logging facility

Syntax

Run the command **logging facility** to configure to record specified error information. To restore to **local7**, run the command **no logging facility**.
logging facility *facility-type*

no logging facility

Parameter

Parameter	Description
facility-type	Facility type Refer to table 3

Default

local7

Command Mode

Global configuration

Usage Guidelines

Table 3 Facility type

Type	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Example

logging facility kern

Related Command

logging console

6.2.5 logging monitor

Syntax

Run the command **logging monitor** to control the information volume displayed on the terminal line
Run the command **no logging monitor** to forbid the log information to be displayed on the terminal line

logging monitor */level*
no logging monitor

Parameter

Parameter	Description
/level	Information level of the logs displayed on the terminal line Refer to table 4

Default

Debugging

Command Mode

Global configuration mode

Usage Guidelines

Table 4 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging monitor errors

Related Command

terminal monitor

6.2.6 logging on

Syntax

Run the command **logging on** to control the recording of error information
Run the command **no logging on** to forbid all records
logging on
no logging on

Parameter

None

Default

logging on

Command Mode

Global configuration mode

Example

switch_config# **logging on**

switch_config# ^Z

switch#

Configured from console 0 by DEFAULT

switch# **ping 192.167.1.1**

switch#ping 192.167.1.1

PING 192.167.1.1 (192.167.1.1): 56 data bytes

!!!!!

--- 192.167.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/4/10 ms

switch#IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending

IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

switch_config# **no logging on**

switch_config# ^Z

switch#

switch# **ping** 192.167.1.1

PING 192.167.1.1 (192.167.1.1): 56 data bytes

!!!!!

--- 192.167.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/4/10 ms

Related Command

logging
logging buffered
logging monitor
logging console

6.2.7 logging trap

Syntax

Run the command **logging trap** to control the information volume recorded to the syslog server
Run the command **no logging trap** to forbid the information to be recorded to the syslog server

logging trap */level*
no logging trap

Parameter

Parameter	Description
/level	Information level of the logs displayed on the syslog server Refer to table 5

Default

Informational

Command Mode

Global configuration mode

Usage Guidelines

Table 5 Level of log recording

Prompt	Level	Description	Syslog Definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

```
logging 192.168.1.1
logging trap notifications
```

Related Command

logging

6.2.8 logging command

Syntax

To enable the command execution recording, run **logging command**. After this function is opened, a log will be generated for each of all entered commands, in which the line to execute this command, the command line, the execution result, the login line and the login address will be recorded
You can use **no logging command** to disable this function

Parameter

None

Default

no logging command

Command Mode

Global configuration mode

Example

Switch_config#logging command
Switch_config#Jul 11 15:26:56 %CMD-6-EXECUTE: `logging command ` return 0, switch(vty 0, 192.168.25.42)

Related Command

logging

6.2.9 logging source-interface

Syntax

This command is used to set the source port of log exchange
You can use **no logging source-interface** to disable this function

Parameter

None

Default

no logging source-interface

Command Mode

Global configuration mode

Example

Switch_config# logging source-interface vlan 1

Related Command

logging

6.2.10 logging history alerts

Syntax

This command is used to set the level of the historical log table to **alerts** (need to act immediately)

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history alerts

Related Command

logging

6.2.11 logging history critical

Syntax

This command is used to set the level of the historical log table to critical

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history critical

Related Command

logging

6.2.12 logging history debugging

Syntax

This command is used to set the level of the historical log table to **debugging**

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history debugging

Related Command

logging

6.2.13 logging history emergencies

Syntax

This command is used to set the level of the historical log table to **emergencies** (system unavailable)

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history emergencies

Related Command

logging

6.2.14 logging history errors

Syntax

This command is used to set the level of the historical log table to **errors**

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history errors

Related Command

logging

6.2.15 logging history informational

Syntax

This command is used to set the level of the historical log table to informational

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history informational

Related Command

logging

6.2.16 logging history notifications

Syntax

This command is used to set the level of the historical log table to **notifications** (normal but important condition)

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history notifications

Related Command

logging

6.2.17 logging history warnings

Syntax

This command is used to set the level of the historical log table to warnings

Parameter

None

Default

logging history warnings

Command Mode

Global configuration mode

Example

Switch_config#logging history warnings

Related Command

logging

6.2.18 logging history rate-limit

Syntax

This command is used to set the log output rate

Parameter

Parameter	Description
<1-512>	Stands for the number of logs which are exported each second

Default

logging history rate-limit 0

Command Mode

Global configuration mode

Example

Switch_config#logging history rate-limit 256

Related Command

logging

6.2.19 logging history size

Syntax

This command is used to set the number of entries in the historical log table

Parameter

Parameter	Description
<0-500>	Stands for the number of historical log entries

Default

logging history size 0

Command Mode

Global configuration mode

Example

Switch_config#logging history size 256

Related Command

logging

6.2.20 service timestamps

Syntax

Run the command **service timestamps** to configure the time stamp that is added when the system is debugged or records the log information

Run the command no **service timestamps** to cancel the time stamp that is added when the system is debugged or records the log information

service timestamps [log|debug] [*uptime*| *datetime*]

no service timestamps [log|debug]

Parameter

Parameter	Description
log	Adds the time stamp before the log information
debug	Adds the time stamp before the debug information
uptime	Duration between the startup of the switch and the current time
datetime	Real-time clock time

Default

Service timestamps log date

Service timestamps debug date

Command Mode

Global configuration mode

Usage Guidelines

The time stamp in the **uptime** form is displayed like HHHH:MM:SS, meaning the duration from the start-up of the switch to the current time

The time stamp in the **date** form is displayed like YEAR-MON-DAY HH:MM:SS, meaning the real-time clock time

Example

Service timestamps debug uptime

6.2.21 clear logging

Syntax

It is used to clear the log information recorded in the memory cache

clear logging

Parameter

None

Command Mode

EXEC mode

Related Command

logging buffered

show logging

6.2.22 show break

Syntax

It is used to display the information about abnormal breakdown of the switch

show break

Parameter

None

Default

None

Command Mode

EXEC mode

Usage Guidelines

It is used to display the information about abnormal breakdown of the switch, helping to find the cause of the abnormality

Example

```
switch#show break
Exception Type:1400-Data TLB error
BreakNum: 1 s date: 2000-1-1    time: 0:34:6
r0          r1          r2          r3          r4          r5          r6
00008538-01dbc970-0054ca18-00000003-80808080-fefefeff-01dbcca1-
r7          r8          r9          r10         r11         r12         r13
00000000-00009032-00000000-7ffffff0-00008588-44444444-0054c190-
r14         r15         r16         r17         r18         r19         r20
000083f4-000083f4-00000000-00000000-00000000-00000000-00000000-
r21         r22         r23         r24         r25         r26         r27
00000000-0000000a-00000001-00000000-00000000-004d6ce8-01dbd15c-
r28         r29         r30         r31         spr8        spr9        ip
00000002-00467078-00010300-00000300-00000310-00008588-00000370-
```

Variables :

00008538-44444444-01dbd15c-01dbcaac-00000002-00000000-004d6ce8-

01dbca18-

00008538 --- do_chram_mem_sys_addr---bspcfg.o

0001060c --- subcmd---cmdparse.o---libcmd.a

000083e4 --- do_chram_mem_sys---bspcfg.o

0000fb24 --- lookupcmd---cmdparse.o---libcmd.a

0000f05c --- cmdparse---cmdparse.o---libcmd.a

003e220c --- vty---vty.o---libvty.a

00499820 --- pSOS_qcv_broadcast---ksppc.o---os\libsys.a

The whole displayed content can be divided into six parts:

1 RROR:file **function.map** not found

The prompt information means that the system has not been installed the software **function.map**, which does not affect the system running

If the version of the software function.map is not consistent with that of the switch, the system prompts that the version is not consistent

2 Exception Type—Abnormal hex code plus abnormal name

3 BreakNum

It is the current abnormal number. It means the number of abnormalities that the system has since it is powered on in the latest time. It is followed by the time when the abnormality occurs

4 Content of the register

The common content of the register is listed out

5 Variable area

The content in the stack is listed out

6 Calling relationship of the number

If the **map** file is not installed on the system, only the function's address is displayed. If the **map** file is installed on the system, the corresponding function name, **.o** file name and .a file name are displayed.

The calling relationship is from bottom to top

6.2.23 show debug

Syntax

It is used to display all the enabled debugging options of the switch

show debug

Parameter

None

Command Mode

EXEC mode

Example

switch# show debug

Crypto Subsystem:

Crypto Ipsec debugging is on

Crypto Isakmp debugging is on

Crypto Packet debugging is on

Related Command

debug

6.2.24 show logging

Syntax

It is used to display the state of logging (syslog)

show logging

Parameter

None

Command Mode

EXEC mode

Usage Guidelines

It is used to display the state of logging (syslog), including the login information about the console, monitor and syslog

Example

switch# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)

Console logging: level debugging, 12 messages logged

Monitor logging: level debugging, 0 messages logged

Buffer logging: level debugging, 4 messages logged

Trap logging: level informations, 0 message lines logged

Log Buffer (4096 bytes):

2000-1-4 00:30:11 Configured from console 0 by DEFAULT

2000-1-4 00:30:28 User DEFAULT enter privilege mode from console 0, level = 15

Related Command

clear logging

Chapter 7 SSH Configuration Commands

7.1 ip sshd enable

Syntax

ip sshd enable

no ip sshd enable

Parameter

None

Default

Disable

Usage Guidelines

It is used to generate the rsa encryption key and then monitor the connection to the ssh server. The process of generating encryption key is a process of consuming the calculation time. It takes one or two minutes

Command Mode

Global configuration mode

Example

In the following example, the SSH service is generated

device_config#ip sshd enable

7.2 ip sshd timeout

Syntax

ip sshd timout time-length

no ip timeout

Parameter

Parameter	Description
time-length	Maximum time from the establishment of connection to the authentication approval Value range: 60-65535

Default

180 seconds

Usage Guidelines

To prevent the illegal user from occupying the connection resources, the connections that are not approved will be shut down after the set duration is exceeded

Command Mode

Global configuration mode

Example

In the following example, the timeout time is set to 360 seconds:

device_config#ip sshd timeout 360

7.3 ip sshd auth-method

Syntax

ip sshd auth-method *method*

no sshd auth-method

Parameter

Parameter	Description
method	Sets authentication method list. The length of the authentication method's name is no more than 20 characters

Default

The default authentication method list is used

Usage Guidelines

The ssh server uses the authentication method list of the login type

Command Mode

Global configuration mode

Example

In the following example, an auth-ssh authentication method list is configured and it is applied to the ssh server:

device_config#aaa authentication login auth-ssh local

device_config#ip sshd auth-method auth-ssh

7.4 ip sshd access-class

Syntax

ip sshd access-class *access-list*

no ip sshd access-class

Parameter

Parameter	Description
access-list	Standard IP access list. The length of the access list's name is no more than 20 characters

Default

No access control list

Usage Guidelines

It is used to configure the access control list for the ssh server. Only the connections complying with the regulations in the access control list can be approved

Command Mode

Global configuration mode

Example

In the following example, an **ssh-accesslist** access control list is configured and applied in the ssh server:

device_config# ip access-list standard ssh-accesslist

device_config_std_nacl#deny 192.168.20.40

device_config#ip sshd access-class ssh-accesslist

7.5 ip sshd auth-retries

Syntax

ip sshd auth-retries *times*

no ip sshd auth-retries

Parameter

Parameter	Description
times	Maximum re-authentication times Value range: 0-65535

Default

6 times

Usage Guidelines

The connection will be shut down when the re-authentication times exceeds the set times

Command Mode

Global configuration mode

Example

In the following example, the maximum re-authentication times is set to five times:
device_config#ip sshd auth-retries 5

7.6 ip sshd clear

Syntax

ip sshd clear *ID*

Parameter

Parameter	Description
ID	Number of the SSH connection to the local device Value range: 0-65535

Default

None

Usage Guidelines

It is used to mandatorily close the incoming ssh connection with the specified number. You can run the command **show ip sshd line** to check the current incoming connection's number

Command Mode

Global configuration mode

Example

In the following example, the No.0 incoming connection is mandatorily closed:

device_config#ip sshd clear 0

7.7 ip sshd silence-period

Syntax

ip sshd silence-period *time-length*

no ip sshd silence-period

Parameter

Parameter	Description

time-length	Means the time of the silence, which ranges from 0 to 3600

Default

60s

Usage Guidelines

This command is used to set the login silence period. After the accumulated login failures exceed a certain threshold, the system regards that there exist attacks and disables the SSH service in a period of time, that is, the system enters the login silence period

The silence period is set by the **ip sshd silence-period** command. The default silence period is 60 seconds. The allowable login failures are set by the **ip sshd auth-retries** command, whose default value is 6

Command Mode

Global configuration mode

Example

The following example shows how to set the silence period to 200 seconds

switch_config#ip sshd silence-period 200

7.8 ip sshd version 2

Syntax

ip sshd version 2

no ip sshd version

Parameter

None

Default

Support ssh v1 and v2 client connection

Usage Guidelines

This command is used to configure the client version that the ssh server allows to log in. After configuration, only v2 version login is supported, and v1 version login is prohibited

Command Mode

Global configuration mode

Example

The following command shows how to configure the ssh server to version 2:

switch_config#ip sshd version 2

7.9 ip sshd Ciphers

Syntax

ip sshd Ciphers *ciphers*

no ip sshd Ciphers

Parameter

Parameter	Description
ciphers	Encryption algorithms list

Default

aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr

Usage Guidelines

This command is used to configure the list of encryption algorithms supported by the ssh server

Command Mode

Global configuration mode

Example

The following command shows how to configure the ssh server to only support the aes256-ctr encryption algorithm:

switch_config#ip sshd Ciphers aes256-ctr

7.9.1 ip sshd KexAlgorithms

Syntax

ip sshd KexAlgorithms *KexAlgorithms*

no ip sshd KexAlgorithms

Parameter

Parameter	Description
KexAlgorithms	Key exchange algorithms list

Default

diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha256

Usage Guidelines

This command is used to configure the list of key exchange algorithms supported by the ssh server

Command Mode

Global configuration mode

Example

The following command shows how to configure the ssh server to only support the diffie-hellman-group-exchange-sha256 key exchange algorithm:
switch_config#ip sshd KexAlgorithms diffie-hellman-group-exchange-sha256

7.10 ip sshd MACs

Syntax

ip sshd MACs *MACs*

no ip sshd MACs

Parameter

Parameter	Description
MACs	Algorithms List of Message Authentication Code

Default

hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96,hmac-sha2-256

Usage Guidelines

This command is used to configure the list of message authentication code algorithms supported by the ssh server

Command Mode

Global configuration mode

Example

The following command shows how to configure the ssh server to only support the hmac-sha2-256 message authentication code algorithm:

switch_config#ip sshd MACs hmac-sha2-256

7.11 ip sshd sftp

Syntax

ip sshd **sftp**

no ip sshd **sftp**

Parameter

None

Default

None

Usage Guidelines

This command is used to enable the SFTP function. The SFTP function refers to the secure file transmission system based on SSH, of which the authentication procedure and data transmission are encrypted. Though it has low transmission efficiency, network security is highly improved

Command Mode

Global configuration mode

Example

The following example shows how to enable the SFTP function

switch_config#ip sshd sftp

7.12 ip sshd save

Syntax

ip sshd save

no ip sshd save

Parameter

None

Default

None

Usage Guidelines

This command is used to save the initial key. When the SSH server is restarted, the key will be first read from the flash; if the key reading is successful, the recalculation of key will be avoided and the startup time will be shortened

Command Mode

Global configuration mode

Example

The following example shows how to enable the key protection function

switch_config#ip sshd save

7.13 ssh

Syntax

ssh –l *userid* **–d** *destIP* **[-c {des|3des|blowfish }] [-o** *numberofpasswdprompts***] [-p** *port***] [-v** {1|2}**] [-s** *password***]**

Parameter

Parameter	Description
–l userid	User account on the server
–d destI	Destination IP address in the dotted decimal system
-o numberofpasswdprompts	Re-authentication times after the first authentication fails Actual re-authentication times is the set value plus the smallest value set on the server. Its default value is three times Value range: 0-65535
-p port	Port number that the server monitors Its default value is 22 Value range: 0-65535
-c {des|3des|blowfish}	Encryption algorithm used during communication The encryption algorithm is 3des by default
-v version	Specified version No
-s password	Set the password

Default

None

Usage Guidelines

The command is used to create a connection with the remote ssh server

Command Mode

Privileged mode

Example

In the following example, a connection with the ssh server whose IP address is 192.168.20.41 is created. The account is zmz and the encryption algorithm is blowfish:

device#ip ssh –l zmz –d 192.168.20.41 –c blowfish

7.14 show ssh

Syntax

show ssh

Parameter

None

Default

None

Usage Guidelines

It is used to display the sessions on the ssh server

Command Mode

Privileged mode

Example

In the following example, the sessions on the ssh server are displayed:

device#show ssh

7.15 show ip sshd

Syntax

show ip sshd

Parameter

None

Default

None

Usage Guidelines

It is used to display the current state of the ssh server

Command Mode

Privileged mode

Example

In the following example, the current state of the ssh server is displayed:

device#show ip sshd

Chapter 8 Virtualization Configuration Commands

8.1 bvss

Syntax

To enter the virtualization configuration mode, run this command

bvss

Parameters

None

Default Value

Disabled

Usage Guidelines

Run this command in configuration mode to enter the virtualization configuration mode. Other virtualization configuration commands must be run in virtualization configuration mode

Example

The following example shows how to enter the virtualization configuration mode

Switch_config#

Switch_config#bvss

Switch_config_bvss#

8.2 bvss enable

Syntax

To enable/disable the virtualization function, run the following commands. The command takes effect when the device restarts up

bvss enable

[no] bvss enable

Parameters

None

Default Value

Disabled

Usage Guidelines

The command can be used when the virtualization function is enabled. The command takes effect only when the virtualization configuration is saved and the device restarts up

Example

The following example shows how to enable the virtualization function:

Switch_config_bvss#

Switch_config_bvss#bvss enable

8.3 bvss domain-id

Syntax

bvss domain-id *id*

To set the virtualization domain and use the domain to differentiate the virtualization group, run this command. One device can only belong to one virtualization domain. Only devices in the same domain can establish the virtualization device.

Parameters

Parameters	Description
id	Stands for the virtualization domain ID, which ranges from 1 to 255

Default Value

Default: 0

Usage Guidelines

The command is configured in the virtualization mode and set the domain ID of the virtualization device. Only devices of the same domain can be virtualized

Example

The following example shows how to set the virtualization domain of the device to 1

Switch_config_bvss#bvss domain-id 1

8.4 bvss member-id

Syntax

To set the member ID of the virtualization device, run the following command. The device within the same domain needs to set with different member IDs

bvss member-id *id*

Parameters

Parameters	Description
id	The member ID of the virtualization device, which ranges from 1 to 4

Default Value

Default: 0

Usage Guidelines

The command must be configured in the virtualization mode. The device within the same domain cannot configure with the same member ID

Example

The following example shows how to set the member ID of the device to 1

Switch_config_bvss# bvss member-id 1

8.5 bvss mode

Syntax

To set the virtualization mode, run this command. The virtualization mode has two types: normal and enhanced. The normal mode only supports the virtualization of two devices and the enhanced mode support virtualization of 4 devices

bvss mode [normal | enhanced]

[no] bvss mode [normal | enhanced]

Parameters

None

Default Value

The default is the independent mode (no virtualization)

Usage Guidelines

The command is set in the virtualization configuration mode. It is the independent mode by default. After the virtualization is enabled, the virtualization mode must configure. At present the device only supports normal mode and enhanced mode. Use the no form of this command to return to the default setting

Example

The following example shows how to set the virtualization to normal mode

Switch_config_bvss#bvss mode normal

8.6 bvss priority

Syntax

To set the priority of the device, run this command. The virtualization protocol is used in negotiating the master device. The device with the highest priority will be selected as the the master device

bvss priority *priority*

[no] bvss priority *priority*

Parameters

Parameters	Description
priority	Means the priority of the device, whose value ranges from 1 to 255

Default Value

Default: 0

Usage Guidelines

The command is used to set the priority of the device in the virtualization configuration mode. The device with the highest priority in the same domain will be negotiated as the master device

Example

The following example shows how to set the priority of the device to 5

Switch_config_bvss#bvss priority 5

8.7 bvss interface

Syntax

To set the virtualization port, run this command. The virtualization port can be used to connect different devices in the same domain

bvss interface *num* **slot** *slot* **port** *port* **group** *group*

no bvss interface *num*

Parameters

Parameters	Description
num	The virtualized port number, which ranges from 1 to 4
slot	The slot number of the virtualization port, which ranges from 0 to 1
Port	The port number of the virtualization port, which ranges from 1 to 8
group	The port group number of the virtualization port, which ranges from 1 to 2

Default Value

None

Usage Guidelines

The command is used to designate the virtualization port in the virtualization configuration mode. The virtualization ports are used to connect different devices and establish the virtualization domain

Example

The following example shows how to configure the virtualization port to g0/1

Switch_config_bvss# bvss interface 1 slot 0 port 1 group 1

8.8 bvss mac-address mode

Syntax

To configure the MAC address of the virtualization system, run this command

bvss mac-address mode [use-active-member | use-static-pool]

Use the mac address of the master device as the virtualization system mac

bvss mac-address mode use-active-member

Use the mac in the reservation address pool as the virtualization system mac

bvss mac-address mode use-static-pool

Parameters

None

Default Value

use-active-member mode

Usage Guidelines

The command is used to configure the virtualization system mac mode in the virtualization configuration mode

Example

The following example shows how to set the mac of the master device to mac of the virtualization system

Switch_config_bvss#bvss mac-address mode use-active-member

8.9 show bvss

Syntax

To show information of virtualization, run this command

show bvss [current-config | running-config l management | statistics | rnp | sgnp | mcpath]

To show the current configuration of virtualization, run the following command. These configurations cannot take effect until they are saved and the device restarts up

show bvss current-config

To show the running configuration of the virtualization, run the following command

show bvss running-config

To show the virtualization management information, runt the following command

show bvss management

To show virtualization statistics information, run the following command

show bvss statistics

To show virtualization role negotiation protocol information, run the following command

show bvss rnp

To show virtualization virtualization group negotiation protocol information, run the following command

show bvss sgnp

To show virtualization non-unicast path information, run the following command

show bvss mcpath

Parameters

None

Default Value

None

Usage Guidelines

The command can be used in the configuration mode or the management mode. It shows the relevant information of the virtualization management

Example

The following example shows how to display the virtualization running configuration, the current configuration and the management information

Switch#show bvss management

bvss management information:

active member: 1, standby member: 2

lgroup: 1-2, rgroup:

orphan group:-1, normal group:-1

HT[l]:, HT[r]: ,HT[a]:

internal topology:0

L to member 1: unknown R to member 1:unknown

L to member 2: 1 R to member 2:unknown

L to member 3: unreachable R to member 3:0

L to member 4: unknown R to member 4:0

hg route

to member 1: local

to member 2: l

to member 3: l

to member 4: error

Switch#show bvss running-config

bvss configuration information:

bvss enable: TRUE

bvss domain-id: 18

bvss member-id : 1

bvss mode: normal

bvss priority: 68

bvss mac-address mode: use-active-member

Switch#show bvss current-config

bvss configuration information:

bvss enable: TRUE

bvss domain-id: 18

bvss member-id : 1

bvss mode: normal

bvss priority: 68

bvss mac-address mode: use-active-member

8.10 debug bvss

Syntax

To debug bvss, run this command

debug bvss [event | message | packet]

To enable the virtualized event debug information, run the following command

debug bvss event

To enable the virtualized message debug information, run the following command

debug bvss message

To enable the virtualized packet debug information, run the following command

debug bvss packet

Parameters

None

Default Value

None

Usage Guidelines

The command is used to show the debug log information of the virtualization module

Example

None

8.11 Configuration Example

The following example shows how to set the virtualization normal mode

bvss enable

bvss mode normal

bvss domain-id 18

bvss member-id 1

bvss priority 68

bvss interface 1 slot 1 port 1 group 1

bvss interface 2 slot 1 port 2 group 1

Chapter 9 CFM Configuration Commands Overview

9.1 Stipulation

9.1.1 Format Stipulation in the Command Line

Syntax	Meaning
Bold	Stands for the keyword in the command line, which stays unchanged and must be entered without any modification. It is presented as a bold in the command line
{italic}	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the brace
<italic>	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the point bracket
[ ]	Stands for the optional parameter, which is in the square bracket
{ x | y | ... }	Means that you can choose one option from two or more options
[x | y | ...]	Means that you can choose one option or none from two or more options
{ x | y | ... } *	Means that you has to choose at least one option from two or more options, or even choose all options
[x | y | ...] *	Means that you can choose multiple options or none from two or more options
&<1-n>	Means that the parameter before the "&" symbol can be entered 1~n times
#	Means that the line starting with the "#" symbol is an explanation line

Chapter 10 CFM

10.1 CFM Configuration Commands

10.1.1 Adding the Maintenance Domain and Entering the Maintenance Domain Mode

Syntax

To add a maintenance domain or enter the already existent maintenance domain, run the following command

ethernet cfm md mdnf *{string}* *<char_string>* [**level** *<0-7>* | **creation** *<MHF_creation_type>* | **sit** *<sender_id_type>* | **ip** *<IP_address>]*

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
level	(optional parameter) Stands for the level of a maintenance domain. It is 0 by default
creation	(optional parameter) Stands for the MIP creation method. It is none by default
sit	(optional parameter) Stands for the type of sender id. It is none by default
ip	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default

Command Mode

Global configuration mode

Example

Switch_config#ethernet cfm md mdnf string customer level 5

Related Command

None

10.1.2 Deleting the Maintenance Domain

Syntax

To delete a designated maintenance domain, run the following command.

no ethernet cfm md mdnf *{string}* *<char_string>*

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive

Command Mode

Global configuration mode

Example

Switch_config#no ethernet cfm md mdnf string customer

Related Command

None

10.1.3 Browsing the Maintenance Domain

Syntax

To browse all the maintenance domains or the designated maintenance domains of the local device, run the following command

show ethernet cfm md [mdnf *{string}* *<char_string>***]**

Parameters

Parameters	Description
mdnf	Stands for the format of the name of a to-be-browsed designated maintenance domain. At present only the char-string format is supported. <char_string> name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive

Command Mode

EXEC, global, interface, maintenance domain

Example

Switch_config#show ethernet cfm md mdnf string customer

Related Command

None

10.1.4 Adding a Maintenance Association

Syntax

To add a maintenance association, run the following command

ma manf *{string}* *<char_string>* *ci {100ms | 1s | 10s | 1min | 10min}* **meps** *<mepids>* [**vlan** *<1-4094>* | **creation** *<MHF_creation_type>* | **sit** *<sender_id_type>* | **ip** *<IP_address>*]

Parameters

Parameters	Description
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> name of the maintenance association. It is in character string mode
ci	Stands for the transmission interval of CCM. The shortest transmission interval which is supported presently is 100ms
meps	Stands for the MEPID of all MEPs in the local maintenance domain
vlan	(optional parameter) Stands for the identifier of the VLAN where the maintenance association is located. It is 1 by default
creation	(optional parameter) MIP It is none by default
sit	(optional parameter) Stands for the identifier type of the sender. It is none by default
ip	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default

Command Mode

Maintenance domain mode

Example

Switch_config_cfm#ma manf string customer1 ci 1s meps 1-2,2009 vlan 10

Related Command

None

10.1.5 Deleting the Maintenance Association

Syntax

To delete a designated maintenance association, run the following command

no ma manf *{string}* *<char_string>*

Parameters

Parameters	Description
manf	Stands for the format of the name of the maintenance association. At present only the char-string

format is supported

<char_string> name of the maintenance association. It is in character string mode

Command Mode

Maintenance domain mode

Example

Switch_config_cfm#no ma manf string customer

Related Command

None

10.1.6 Browsing the Maintenance Association

Syntax

To browse all or designated maintenance associations in a designated maintenance domain on the local device, run the following command.

show ethernet cfm ma mdnf *{string} <char_string>* [**manf** {string} <char_string>]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain where the to-be-browsed maintenance association is located. At present only the char-string format is supported. <char_string> the name of the maintenance domain where the to-be-browsed maintenance association is located. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of a to-be-browsed maintenance association. At present only the char-string format is supported <char_string> the name of a to-be-browsed maintenance association. It is in character string mode

Command Mode

EXEC, global, interface, maintenance domain

Example

Switch_config#show ethernet cfm ma mdnf string customer manf string customer1

Related Command

None

10.1.7 Adding MIP

Syntax

To add an MIP of a specific level, which belongs to a designated VLAN, on a specific interface, run the following command.

ethernet cfm mip add level *<0-7>* [*vlan <1-4094>*]

Parameters

Parameters	Description
level	Stands for the level of a maintenance domain
vlan	Stands for the identifier of the VLAN where the maintenance association is located. It is 1 by default

Command Mode

Physical interface configuration mode

Example

Switch_config_g0/1#ethernet cfm mip add level 1 vlan 10

Related Command

None

10.1.8 Deleting MIP

Syntax

To delete a designated MIP, run the following command

ethernet cfm mip del vlan *< 1-4094>*

Parameters

Parameters	Description
vlan	Stands for the identifier of the VLAN where MIP is located

Command Mode

Interface configuration mode

Example

Switch_config_g0/1#ethernet cfm mip del vlan 10

Related Command

None

10.1.9 Browsing MIP

【Method 1】

Syntax

To browse all MIPs of a designated interface in the local device or MIPs in a specific VLAN, run the following command

show ethernet cfm mip vlan <*1-4094*> **interface** <*interface_name*>

show ethernet cfm mip interface <*interface_name*>

Parameters

Parameters	Description
interface	Stands for a to-be-browsed interface
vlan	Stands for the identifier of a to-be-browsed VLAN

Command Mode

EXEC, global, interface, maintenance domain

Example

Switch_config#show ethernet cfm mip vlan 1 interface g0/1

Related Command

None

【Method 2】

Syntax

To browse all MIPs on the current interface of the local device, run the following command

ethernet cfm mip display

Parameters

None

Command Mode

Physical interface mode

Example

Switch_config_g0/1#ethernet cfm mip display

Related Command

None

10.1.10 Adding MEP

Syntax

To add an MEP, which belongs to a designated maintenance association, on a specific interface, run the following command

ethernet cfm mep add mdnf *{string} <char_string>* **manf** *{string} <char_string>* **mepid** *<1-8191>* **rmepid** *<1-8191>* [**direction** *{up | down}* | **ip** *<ip_address>* | **lap** *{all | mac | rCCM | eCCM | xcon | none}* | **fat** *<250 - 1000>* | **frt** *<250 - 1000>*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the to-be-added MEP
rmepid	Stands for the MEPID of the remote MEP
direction	(optional parameter) Stands for the direction of the to-be-added MEP. It is down by default
ip	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default
lap	(optional parameter) Stands for the lowest priority of trouble report. It is all by default
fat	(optional parameter) Failure appearance duration, range: 250-1000 (unit: 10ms)
frt	(optional parameter) Failure recovery interval, range: 250-1000 (unit: 10ms)

Command Mode

Physical interface configuration mode

Example

Switch_config_g0/1#ethernet cfm mep add mdnf string customer manf string customer1 mepid 2009 rmepid 2008 direction up lap all fat 500 frt 500

Related Command

None

10.1.11 Deleting MEP

Syntax

To delete a designated MEP, run the following command

ethernet cfm mep del mdnf *{string}* *<char_string>* **manf** *{string}* *<char_string>* **mepid** *<1-8191>*

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the to-be-removed MEP

Command Mode

Physical interface configuration mode

Example

Switch_config_g0/1#ethernet cfm mep del mdnf string customer manf string customer1 mepid 2009

Related Command

None

10.1.12 Browsing MEP

【Method 1】

Syntax

To browse the detailed or brief information about all MEPs in the designated maintenance domain of the local device, or that about a specific MEP, run the following command

show ethernet cfm mep mdnf *{string}* *<char_string>* **manf** *{string}* *<char_string>* [**mepid** *<1-8191>*] [**view** *{detail | brief}*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the to-be-browsed MEP
view	Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default

Command Mode

EXEC, global, interface, maintenance domain

Example

Switch_config#show ethernet cfm mep mdnf string x manf string x view brief

Related Command

None

【Method 2】

Syntax

To browse all MEPs on the current interface of the local device, run the following command

ethernet cfm mep display

Parameters

None

Command Mode

Physical interface mode

Example

Switch_config_g0/1#ethernet cfm mep display

Related Command

None

10.2 CFM Maintenance Commands

10.2.1 Loopback

Syntax

To use a designated MEP at the local terminal to conduct loopback towards another designated MEP at the remote terminal, run the following command

ethernet cfm loopback mdnf *{string}* *<char_string>* **manf** *{string}* *<char_string>* **mepid** *<1-8191>* **mac** *<AA:BB:CC:DD:EE:FF>* [**number** *<1-64>*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the local MEP
mac	Stands for the MAC address of the remote MEP
number	(optional parameter) Stands for the times of conducting loopback. It is 3 by default

Command Mode

EXEC

Example

Switch#ethernet cfm loopback mdnf string x manf string x mepid 1 mac 00:15:E9:43:AD:E3 number 3

Related Command

None

10.2.2 Linktrace

Syntax

To use a designated local MEP to conduct linktrace towards a designated remote MEP, run the following command

ethernet cfm linktrace mdnf *{string}* *<char_string>* **manf** *{string}* *<char_string>* **mepid** *<1-8191>* **mac** *<AA:BB:CC:DD:EE:FF>* [**ttl** *{1-255}* | **fdb-only** *{yes}*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the local MEP
mac	Stands for the MAC address of the remote MEP
ttl	(optional parameter) Stands for the tt1 value. It is 64 by default
fdb-only	(optional parameter) Stands for whether LTM forwarding is used only with the MAC address table. It is yes by default

Command Mode

EXEC

Example

Switch#ethernet cfm linktrace mdnf s x manf string x mepid 1 mac 00:15:E9:43:AD:E3 ttl 64

Related Command

None

10.2.3 Deleting the Linktrace Result Table

Syntax

To delete the linktrace result table of a designated MEP, run the following command

clear ethernet cfm linktrace mdnf *{string}* *<char_string>* **manf** *{string}* *<char_string>* [**mepid** *<1-8191>*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42

	printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the local MEP

Command Mode

EXEC

Example

Switch#clear ethernet cfm linktrace mdnf string x manf string x mepid 1

Related Command

None

10.2.4 Setting the Size of the Linktrace Result Table

Syntax

To set the size of the linktrace result table (that is, the number of linktraces which can be conducted concurrently), run the following command

ethernet cfm linktrace table-size *<1-16>*

Parameters

Parameters	Description
table-size	Stands for the size of the linktrace result table

Command Mode

Global configuration mode

Example

Switch_config#ethernet cfm linktrace table-size 1

Related Command

None

10.2.5 Setting the Number of Entries in the Linktrace Result Table

Syntax

To set the maximum number of entries that are received each time by the linktrace result table, run the following command

ethernet cfm linktrace entry-number *<2-4095>*

Parameters

Parameters	Description
entry-number	Stands for the number of the entries in the linktrace result table

Command Mode

Global configuration mode

Example

Switch_config#ethernet cfm linktrace entry-number 2009

Related Command

None

10.2.6 Setting the Aging Time of the Linktrace Result Table

Syntax

To set the maximum number of entries that are received each time by the linktrace result table(Unit:min), run the following command

ethernet cfm linktrace hold-time *<1-29>*

Parameters

Parameters	Description
hold-time	Stands for the aging time of the linktrace result table. Unit: minute

Command Mode

Global configuration mode

Example

Switch_config#ethernet cfm linktrace hold-time 10

Related Command

None

10.2.7 Deleting the MEP Statistics Data

Syntax

To delete the statistics data of a designated MEP, run the following command

ethernet cfm mep clear mdnf *{string}* *<char_string>* **manf** *{string}* *<char_string>* **mepid** *<1-8191>*

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of a designated MEP

Command Mode

Physical interface mode

Example

Switch_config_g0/1#ethernet cfm mep clear mdnf string x manf string x mepid 1

Related Command

None

10.3 CFM Control Commands

10.3.1 CFM Stack Control Command

Syntax

ethernet cfm *{enable | disable}*

To enable or disable the whole CFM protocol stack, run the followingcommand

Parameters

None

Command Mode

Global configuration mode

Example

Switch_config#ethernet cfm enable

Related Command

None

10.3.2 CFM Interface Control Command

Syntax

To enable or disable the CFM function of the current interface, run the following command

ethernet cfm *{enable | disable}*

Parameters

None

Command Mode

Physical interface mode

Example

Switch_config_g0/1#ethernet cfm enable

Related Command

None

10.3.3 MIP Control Command

Syntax

To enable or disable the MIP of a designated VLAN on the current interface, run the following command

ethernet cfm mip *{enable | disable}* **vlan** *<1-4094>*

Parameters

None

Command Mode

Physical interface mode

Example

Switch_config_g0/1#ethernet cfm mip enable vlan 1

Related Command

None

10.4 CFM Query Commands

10.4.1 Browsing the CFM Protocol Stack

Syntax

To browse the CFM protocol stack, run the following command

show ethernet cfm stack

Parameters

None

Command Mode

Non-user mode

Example

Switch_config#show ethernet cfm stack

Related Command

None

10.4.2 Browsing the CFM Interface

Syntax

The command is used to check the relevant information of CFM interface

show ethernet cfm interface [*<interface_name>*]

Parameters

None

Command Mode

Non-user mode

Example

Switch_config#show ethernet cfm interface g0/1

Related Command

None

10.4.3 Browsing the Locally Stored Information about the Remote MEP

Syntax

To browse the detailed or brief information about all remote MEPs, which together with a designated local MEP belong to the same maintenance association, or about a designated remote MEP, run the following command

show ethernet cfm rmep mdnf *{string} <char_string>* **manf** *{string} <char_string>* [**mepid** *<1-8191>*] [**rmepid** *<1-8191>*] [**view** {*detail | brief*}]

Parameters

Parameters	Description

mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported <char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association
rmepid	Stands for the MEPID of the to-be-browsed remote MEP
view	Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default

Command Mode

Non-user mode

Example

Switch_config#show ethernet cfm rmep mdnf string x manf string x mepid 1 rmepid 2 view brief

Related Command

None

10.4.4 Browsing the LinkTrace Result Table

Syntax

To browse the linktrace result table which is carried out by a specified TID of a specific MEP, run the following command

show ethernet cfm linktrace mdnf *{string} <char_string>* **manf** *{string} <char_string>* **mepid** *<1-8191>* **tid** *<0-4294967295>*

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported <char_string> the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported

	<char_string> the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive
mepid	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association
tid	Stands for the TID that is returned during linktrace

Command Mode

Non-user mode

Example

Switch_config#show ethernet cfm linktrace mdnf string x manf string x mepid 1 tid 19830719

```
**** [RESULT FOR READING LINKTRACE REPLY] ****

                ================================================
                                ID :0x12E97BF (19830719)【Event ID of the presently running LT】
                                TTL :0x00000004(4)  【TTL value of the presently running LT】
                            TOTAL LTRs:1【LTRs returned by the remote terminal of the result table】
                              MAX LTRs:100【receiving at most 100 LTRs】
                            NEXT ORDER:2【The next expected LTR order ID】

                                【The total information of one Linktrace is shown above】
                ==================== LTRs ====================

                                order:1【Order ID of this LTR】
                                  TTL:3【TTL vlaue in the responsed LTRs】
                                FwdYes:NO【Whether the local node forwards LTM】
                             TerminalMEP:NO【Whether the local node is the terminal MEP】
                          Last Egress ID:0 - 00:E0:0F:DC:02:11【MAC of the previous hop】
                          Next Egress ID:0 - 00:00:00:00:00:00【MAC of the next hop, and if the result is 0 it means there is no
next hop】
                            Relay Action:(1)HIT【Field of the Relay action: HIT means just hitting successively】
                          Ingress Action:OK(1)【state of the ingress port: OK】
                       Ingress MAC Address:00:E0:0F:81:11:1C【MAC of the ingress port】
                    Ingress Port ID format:MAC-ADDRESS(3)【ID format of the ingress port: MAC format】
                     Ingress Port ID (hex):00 E0 0F 81 11 1C【Identifier of the ingress port：00 E0 0F 81 11 1C】
```

Related Command

None

10.4.5 Browsing the Whole Running Status of CFM

Syntax

To browse the whole running status of CFM, run the following command

show ethernet cfm running-info

Parameters

None

Command Mode

Non-user mode

Example

Switch_config#show ethernet cfm running-info

Related Command

None

10.5 Y.1731 Command

10.5.1 Enable frame delay measurement function

Syntax

To enable frame delay measurement function, unidirectional or bidirectional mode, run the following command

ethernet y1731 delay-measurement [**-n** *number*]* *MEGID* {**aimmep** *MEPID*| *macaddr* } [**one-way**]

Parameters

Parameters	Description
-n	Optional parameter to set the number of packets to send, the default value is 5 (only valid for bidirectional detection)
MEGID	Stands for the name of MEG, which is a character string with a length of 1 to 13
aimmep	Stands for the destination mep that performs the frame delay measurement function, needs to learn the mac address of the destination mep through the cc function
macaddr	Stands for the MAC address of the destination MEP that performs the frame delay measurement function, does not need to learn the MAC address
one-way	Stands for executing the one-way frame delay measurement function, and will continuously send one-way delay measurement messages after enabled

Command Mode

EXEC

Example

Switch#ethernet y1731 delay-measurement testaa 1234.5678.9abc

Two-way delay measurement MEG: testaa Local MEP: 1 Aimaddress: 1234.5678.9ABC

-- delay measurement statistics--

Packets: send = 5, Received = 5, Lost = 0(0/5 loss)

-- Approximate round trip times in milli-seconds:

MINFD = -2545510ms, MAXFD = -2545440ms, Average = 856447987ms

MINFDV = 0ms, MAXFDV = 20ms

Switch#

Related Command

None

10.5.2 Show the statistics about the one-way delay measurement received locally

Syntax

To show the statistics about the one-way delay measurement, which is locally received, run the following command

show ethernet y1731 delay-measurement *MEGID*

Parameters

Parameters	Description
MEGID	Stands for the name of MEG, which is a character string with a length of 1 to 13

Command Mode

Non-user mode

Example

The following example shows how to display the statistics of the one-way delay measurement of MEG aaa:

Switch#show ethernet y1731 delay-measurement aaa

MEG one way delay measurement :

FD min: 1708520ms

FD max: 1708540ms

Average FD: 1708530ms

FDV current: 0ms

FDV min: 0ms

FDV max: 0ms

Switch#

Related Command

None

10.5.3 Show the statistical information of the Y.1731 module

Syntax

To show the statistical information of the Y.1731 module, including statistics of receiving and sending OAM packets and statistics of system errors, run the following command

show ethernet y1731 traffic

Parameters

None

Command Mode

Non-user mode

Example

Switch_config#

Switch_config#show ethernet y1731 traffic

ethernet y1731 traffic/errors:

Total output CCM frames: 223933

Total output LBM frames: 67

Total output LTM frames: 41

Total output AIS frames: 0

Total output 1DM frames: 1067

Total output DMM frames: 60

Total input CCM frames: 160778

Total input LBM frames: 30

Total input LBR frames: 67

Total input LTM frames: 0

Total input LTR frames: 41

Total input AIS frames: 0

Total input 1DM frames: 0

Total input DMM frames: 0

Total input DMR frames: 60

Total memory allocation failures: 0

Total system failures: 0

Switch_config#

Related Command

None

10.5.4 Deleting the Statistics Information about the One-Way Delay Measurement Carried Out by a Designated MEG

Syntax

To delete the statistics information about the one-way delay measurement carried out by a designated MEG, run the following command

clear ethernet y1731 delay-measurement *MEGID*

Parameters

Parameters	Description
MEGID	Stands for the name of MEG, which is a character string with a length of 1 to 13

Command Mode

EXEC

Example

The following example shows how to delete the statistics information about the one-way delay measurement carried out by MEG aaa

Switch#clear ethernet y1731 delay-measurement aaa

Related Command

None

10.5.5 Deleting the Transmission Statistics Information about the OAM Packets and the System Error Information

Syntax

To delete the transmission statistics information about the OAM packets and the system error information, run the following command

clear ethernet y1731 counters

Parameters

None

Command Mode

EXEC

Example

The following example shows how to delete the statistics information about the one-way delay measurement carried out by MEG aaa

Switch#clear ethernet y1731 counters

Related Command

None

Chapter 11 DHCP-Relay Snooping Configuration Commands

11.1 ip dhcp-relay snooping

Syntax

ip dhcp-relay snooping

no ip dhcp-relay snooping

To enable or disable the DHCP-relay snooping function in a VLAN, run **ip dhcp-relay snooping**. To resume the corresponding default settings, run **no dhcp-relay snooping**

Parameter

None

Default

The dhcp-relay snooping function is disabled by default.

Usage Guidelines

None

Example

The following example shows how to enable the DHCP-relay snooping function:

Switch_config#ip dhcp-relay snooping

Switch_config#

11.2 ip dhcp-relay snooping vlan

Syntax

ip dhcp-relay snooping vlan *vlan_id*

no ip dhcp-relay snooping vlan *vlan_id*

Parameter

Parameter	Description
vlan id	ID of a VLAN Range: 1-4094

Default

None

Usage Guidelines

This command is used to configure the VLAN of DHCP snooping

Example

The following example shows how to conduct the snooping inspection to the DHCP packets in VLAN2

switch(config)# ip dhcp-relay snooping vlan 2
switch(config)#

11.3 ip dhcp-relay snooping vlan *vlan_id* max-client

Syntax

ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*

no ip dhcp-relay snooping vlan *vlan_id* **max-client**

Parameter

Parameter	Description
vlan_id	VLAN id. The value ranges from 1 to 4094.
number	The max user number: 0~65535

Default

The max user number is 65535 by default

Usage Guidelines

You can use this command to set the maximum users in a VLAN of DHCP snooping. During this settings, the principle "first come and first be distributed" will be followed. When the number of users in the VLAN reaches the maximum value, new clients are then forbidden to distribute

Example

The following example shows how to set snooping detection for DHCP packets on VLAN 2 and the number of maximum users is 3

Switch_config#ip dhcp-relay snooping vlan 2 max-client 3

Switch_config#

11.4 ip dhcp-relay snooping database-agent

Syntax

ip dhcp-relay snooping database-agent *A.B.C.D*

no ip dhcp-relay snooping database-agent *A.B.C.D*

To configure the TFTP server for backing up DHCP-snooping binding, run **ip dhcp-relay snooping database-agent** ***A.B.C.D***

Parameter

Parameter	Description
A.B.C.D	Stands for the IP address of the TFTP server

Default

There is no standby servers by default

Usage Guidelines

If the address of the TFTP server is not configured, the binding backup is not conducted

Example

The following example shows how to set the address of a server of backing up DHCP snooping binding to 192.168.1.1

Switch_config#ip dhcp-relay snooping database-agent 192.168.1.1

Switch_config#

11.5 ip dhcp-relay snooping db-file

Syntax

ip dhcp-relay snooping db-file *name [timestamp]*

no ip dhcp-relay snooping db-file *[timestamp]*

Parameter

Parameter	Description
Name	File name which is saved during DHCP snooping binding backup
timestamp	File name which is saved with timesatmp

Default

There is no file

Usage Guidelines

If the file name is not configured, the binding backup is not conducted

Example

The following example shows how to set the file name of binding backup to **dhcp_binding.txt**

switch(config)# ip dhcp-relay snooping db-file dhcp_binding.txt

switch(config)#

11.6 ip dhcp-relay snooping write-time

Syntax

ip dhcp-relay snooping write-time *num*

no ip dhcp-relay snooping write-time

Parameter

Parameter	Description
Num	Stands for the interval of backing up the DHCP snooping binding

Default

The Default of the interval is 30 minutes

Usage Guidelines

The binding update will be checked during interval configuration. If the binding is updated, the binding information need be backed up

Example

The following example shows how to set the interval of backing up the binding to 60 minutes

switch(config)# ip dhcp-relay snooping write 60

switch(config)#

11.7 ip dhcp-relay snooping write-immediately

Syntax

ip dhcp-relay snooping write-immediately

no ip dhcp-relay snooping write-immediately

Parameter

None

Default

None

Usage Guidelines

The command enables the item update is immediately written into the binding item database. It is recommended that do not enable the function when there are many items

Example

The following example shows how to back up the binding item immediately after its configuration item is updated

Switch_config#ip dhcp-relay snooping write-immediately

Switch_config#

11.8 ip dhcp-relay snooping log

Syntax

ip dhcp-relay snooping log

no ip dhcp-relay snooping log

Parameter

None

Default

None

Usage Guidelines

After this function is enabled, if there are any packet of dhcp server in the untrust port, the syslog indicates that there is an illegal dhcp server

Example

The following example shows how to enable the log function of dhcp snooping

Switch_config#ip dhcp-relay snooping log

Switch_config#

11.9 ip dhcp-relay snooping rapid-refresh-bind

Syntax

ip dhcp-relay snooping rapid-refresh-bind

no ip dhcp-relay snooping rapid-refresh-bind

To enable dhcp snooping rapid refresh item function, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

None

Default

None

Usage Guidelines

After this function is enabled, the DHCP attack of fake MAC will be closed; when the client is allowed to change the access port, the IP address can be directly acquired without waiting for the expiration of the IP lease

After this function is enabled, if the client changes its access port, the device with snooping enabled will take it as the dhcp packet attack of the fake mac and drop the dhcp packets

Example

None

11.10 dhcp-relay snooping information option

Syntax

ip dhcp-relay snooping information option [format snmp-ifindex | manual | cm-type | hn-type [host] | hw-type]

no ip dhcp-relay snooping information option [format snmp-ifindex | manual | cm-type | hn-type [host] | hw-type]

Parameter

Parameter	Description
format snmp-ifindex	Fills in option 82 in SNMP **ifindex** mode (optional)
format manual	Fills in option 82 manually (optional)
format cm-type	Fills in option 82 in **cm-type** mode (optional)
Format hn-type [host]	Fills in option 82 in **cisco** mode (optional) Host stands for the main switch
format hw-type	Fills in option 82 in **hw-type** mode (optional)

Default

Option 82 will not be added to or removed from the report by default

Usage Guidelines

This command is used to set whether DHCP option82 can be handled when a switch is conducting DHCP snooping. If format snmp-ifindex is designated, Use the SNMP ifindex mode to fill in option 82; otherwise, fill in option 82 according to RFC3046

Example

The following example shows how to fill in option 82 in SNMP ifindex mode:

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping information option format snmp-ifindex

The following example shows how to fill in option 82 in **manual** mode:

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan [WORD] //[WORD] is the vlan name that means need for enable snooping function

Switch_config# ip dhcp-relay snooping information option format manual

11.11 ip verify source vlan

Syntax

ip verify source vlan *vlanid*

no ip verify source vlan *vlanid*

Parameter

Parameter	Description
vlan id	ID of a VLAN Range: 1-4094

Default

None

Usage Guidelines

This command is used to configure a VLAN for monitoring the source IP address. The "no" form of this command is used to cancel this VLAN. If the source IP and source MAC of the IP packet are not the legal client address assigned by the dhcp server monitored by dhcp snooping, then such a packet is regarded as an illegal packet in the vlan with IP source address monitoring enabled, and the packet is discarded Text

Example

The following example shows how to conduct source IP address monitoring to the packets from all physical interfaces (except trusted interfaces) in VLAN2

switch(config)# ip verify source vlan 2
switch(config)#

11.11.1 ip arp inspection vlan

Syntax

ip arp inspection vlan *vlanid*

no ip arp inspection vlan *vlanid*

Parameter

Parameter	Description
vlan id	Queries the time of the timer. Range: 1-4094

Default

None

Usage Guidelines

This command is used to configure a VLAN for monitoring the source address of the ARP packet. The "no" form of this command is used to cancel this VLAN. Under the VLAN that enables ARP packet source address monitoring, ARP packets with SIP and SMAC corresponding to the IP address and mac address assigned by the dhcp server to the client are discarded

Example

The following example shows how to conduct source address monitoring to the ARP packets from all physical interfaces (except trusted interfaces) in VLAN2

Switch_config#ip arp inspection vlan 2

Switch_config#

11.12 ip source binding

Syntax

ip source binding *xx:xx:xx:xx:xx:xx A.B.C.D* **interface** *name* **vlan** *vlan-id*

no ip source binding *xx:xx:xx:xx:xx:xx A.B.C.D* **vlan** *vlan-id*

To add MAC-to-IP binding to an interface, run **ip source binding** ***xx-xx-xx-xx-xx-xx A.B.C.D*** **interface** ***name***

Parameter

Parameter	Description
xx-xx-xx-xx-xx-xx	MAC address
A.B.C.D	IP address
Name	Name of the interface
vlan-id	vlan id nunber

Default

None

Usage Guidelines

None

Example

The following example shows how to bind MAC address **08:00:3e:00:00:01** to IP address **192.168.1.2** on interface GigaEthernet0/1

Switch_config#ip source binding 08:00:3e:00:00:01 192.168.1.2 interface GigaEthernet0/1

Switch_config#

11.13 arp inspection trust

Syntax

arp inspection trust

no arp inspection trust

Parameter

None

Default

The interfaces are distrusted ones by default

Usage Guidelines

The ARP monitoring is not conducted to the ARP-trusted interface. The "no" form of this command is used to configure the Default of this interface

Example

The following example shows how to set interface GigaEthernet0/1 to an ARP-trusted interface

Switch_config_g0/1#arp inspection trust

11.14 dhcp snooping trust

Syntax

dhcp snooping trust

no dhcp snooping trust

Parameter

None

Default

The default interface is a distrusted one

Usage Guidelines

DHCP snooping is not conducted to the DHCP-trusted interface. The "no" form of this command is used to resume the Default of this interface

Example

The following example shows how to set interface GigaEthernet0/1 to a DHCP-trusted interface

Switch_config_g0/1#dhcp snooping trust

11.15 dhcp snooping deny

Syntax

dhcp snooping deny

no dhcp snooping deny

Parameter

None

Default

DHCP snooping is allowed on the default interface

Usage Guidelines

After this command is configured, DHCP snooping trust, IP-sourcetrust and ARP inspection trust are automatically enabled. The "no" form of this command is used to configure the Default of this interface

Example

The following example shows how to disable DHCP snooping on interface GigaEthernet0/1

Switch_config_g0/1#dhcp snooping deny

11.16 dhcp snooping information circuit-id

Syntax

dhcp snooping information circuit-id {string *STRING* **| hex** *xx-xx-xx-xx-xx-xx***}**

Parameter

Parameter	Description
string *STRING*	Stands for the character string carried by the sub-option of option82 circuit-id
hex *xx-xx-xx-xx-xx-xx*	Stands for the Hex system carried by option82 circuit-id

Default

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set option82 need be enabled. See the command, **ip dhcp-relay snooping information option format manual**)

Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

Switch_config#ip dhcp-relay snooping information option format manual

Switch_config#interface g0/3

Switch_config_g0/3#dhcp snooping information circuit-id string group1

11.17 dhcp snooping information remote-id string

Syntax

dhcp snooping information remote-id {string *STRING* **| hex** *xx-xx-xx-xx-xx-xx***}**

Parameter

Parameter	Description
string STRING	Stands for the character string carried by the sub-option of option82 remote-id
hex xx-xx-xx-xx-xx-xx	Stands for the Hex system carried by option82 remote-id

Default

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (The switch of manually set option82 need be enabled. See the command, **ip dhcp-relay snooping information option format manual**)

Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3.

Switch_config# ip dhcp-relay snooping

Switch_config# ip dhcp-relay snooping vlan 1

Switch_config#ip dhcp-relay snooping information option format manual

Switch_config#interface g0/3

Switch_config_g0/3# dhcp snooping information remote-id string group1

11.18 dhcp snooping information vendor-specific

Syntax

dhcp snooping information vendor-specific { string *STRING* **| hex** *xx-xx-xx-xx-xx-xx* **}**

Parameter

Parameter	Description
string STRING	**Stands for the character string carried by the sub-option of option82 verdor-specific**
hex xx-xx-xx-xx-xx-xx	**Stands for the Hex system carried by option82 verdor-specific**

Default

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (The switch of manually set option82 need be enabled. See the command, **ip dhcp-relay snooping information option format manual**)

Example

The following example shows how to set vendor-specific (suboption 9) of option 82 by the hex system on interface g0/3

Switch_config# ip dhcp-relay snooping

Switch_config# ip dhcp-relay snooping vlan 1

Switch_config#ip dhcp-relay snooping information option format manual

Switch_config#interface g0/3

Switch_config_g0/3# dhcp snooping information vendor-specific hex 00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34

11.19 dhcp snooping information append

Syntax

dhcp snooping information append

dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| hostname | vlanip }**

dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| hostname | vlanip }**

no dhcp snooping information append

no dhcp snooping information append first-subop9-param

no dhcp snooping information append second-subop9-param

Parameter

Parameter	Description
first-subop9-param hex [*xx-xx-xx-xx-xx-xx*]	Stands for the Hex system of the first parameter carried by option82 vendor-specific (suboption9)
second-subop9-param hex [*xx-xx-xx-xx-xx-xx*]	Stands for the Hex system of the second parameter carried by option82 vendor-specific (suboption9)
hostname	Stands for the host name carried by option82 vendor-specific (suboption9)
vlanip	Stands for the IP address of the interface vlan carried by option82 vendor-specific (suboption9)

Default

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping

This command without parameters acts as a switch command. When append is enabled, the information of this command will be added to suboption9 of option82. The added information is first-subop9-param and second-subop9-param

Example

The following example shows how to expand the packet with option82 on interface g0/3 and add parameter 1 for suboption9 with the hex system 61-62-63-61-62-63

Switch_config_g0/3# dhcp snooping information append

Switch_config_g0/3#dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
61-62-63-61-62-63 is the hex system for the added parameter

11.20 dhcp snooping information drop

Syntax

dhcp snooping information drop

no dhcp snooping information drop

Parameter

None

Default

None

Usage Guidelines

This command can be set on each port that connects the client

After this command is set, the request packets that contain option82 will be dropped on the stipulated port

Example

The following example shows how to drop the dhcp packet with option82 on interface g0/3

Switch_config_g0/3# dhcp snooping information drop

11.21 ip-source trust

Syntax

ip-source trust

no ip-source trust

Parameter

None

Default

The default interface is a distrusted one

Usage Guidelines

Source IP address snooping is not conducted to the source-IP-trusted interface. The "no" form of this command is used to resume the Default of this interface

Example

The following example shows how to set interface GigaEthernet0/1 to a source-ip-trusted interface

Switch_config_g0/1#ip-source trust

11.22 show ip dhcp-relay snooping

Syntax

show ip dhcp-relay snooping

Parameter

None

Default

None

Usage Guidelines

This command is used to display the information about DHCP-relay snooping configuration

Example

The following example shows how to display the information about DHCP-relay snooping configuration

Switch_config#show ip dhcp-relay snooping

11.23 show ip dhcp-relay snooping binding

Syntax

show ip dhcp-relay snooping binding [all]

Parameter

None

Default

None

Usage Guidelines

This command is used to display the binding information about DHCP-relay snooping

If the **all** parameter is in the command sentence, all binding information about DHCP-relay snooping will be displayed

Example

The following example shows how to display the binding information about DHCP-relay snooping

Switch_config#show ip dhcp-relay snooping binding

11.24 debug ip dhcp-relay snooping

Syntax

debug ip dhcp-relay snooping

no debug ip dhcp-relay snooping

Parameter

None

Default

None

Usage Guidelines

This command is used to enable or disable the debugging switch of DHCP-relay snooping

Example

The following example shows how to enable the debugging switch of DHCP-relay snooping

Switch#debug ip dhcp-relay snooping

Switch#

11.25 debug ip dhcp-relay event

Syntax

debug ip dhcp-relay eventr

no debug ip dhcp-relay event

Parameter

None

Default

None

Usage Guidelines

This command is used to enable or disable the event debugging switch of DHCP-relay

Example

The following example shows how to enable the event debugging switch of DHCP-relay

Switch#debug ip dhcp-relay event
Switch#

11.26 debug ip dhcp-relay binding

Syntax

debug ip dhcp-relay binding

no debug ip dhcp-relay binding

Parameter

None

Default

None

Usage Guidelines

This command is used to enable or disable the binding debugging switch of DHCP-relay snooping

Example

The following example shows how to enable the binding debugging switch of DHCP-relay snooping

Switch#debug ip dhcp-relay binding

Switch#

Chapter 12 DoS Attack Prevention Configuration Commands

12.1 dos enable

Syntax

dos enable {all /icmp *icmp-value* **| ip | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value* **| tcpsmurf | icmpsmurf | ipsmurf }**

no dos enable { **all /icmp** *icmp-value* **| ip | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value* **| tcpsmurf | icmpsmurf | ipsmurf** }

Parameter

Parameter	Description
all	Enables to prevent all kinds of DoS attacks
icmp *icmp-value*	Enables to check ICMP messages. The maximum length of ICMP message is *icmp-value*. ICMP and ICMPv6 messages with length greater than icmp-value will be discarded
ip	Enables to prevent the dos attack messages whose source IP address is same as its destination IP address
l4port	Enables to check the layer-4 messages whose source port is same as its destination port
mac	Enables to prevent the messages whose source MAC address is same as its destination MAC address
tcpflags	Starts to check the TCP packets with illegal flags
tcpfrag tcpfrag-value	Enables to check dos attack messages of tcp subcontract, the minimum tcp header is *tcpfrag-value*, the default value is 20
tcpsmurf	Enables to prevent TCP messages whose destination address is broadcast address
icmpsmurf	Enables to prevent ICMP messages whose destination address is broadcast address
ipsmurf	Enables to prevent IP messages whose destination address is broadcast address

Default

DoS attack prevention is disabled by default

Usage Guidelines

DoS attack prevention is configured in global mode

The ip sub-function can defend against LAND attack, preventing IP messages whose source address is the same

as destination address

The icmp sub-function can drop packets: 1. ICMP 、ICMPv6 ping request message that is large than *icmp-value*; 2. Subcontact ICMP、ICMPv6 message. It can defend against PING attack

The l4port sub-function can drop TCP/UDP packets whose source port number is the same as destination port number

The mac sub-function can check MAC address, preventing messages whose source MAC address is the same as destination MAC address

The tcpflags sub-function can drop the following 4 kinds of TCP packets: 1.TCP SYN flag = 1 & source port<1024； 2.TCP control flags = 0 & sequence = 0； 3.TCP FIN URG PSH =1 & sequence = 0； 4.TCP FIN SYN =1

The tcpfrag sub-function can drop the following 2 kinds of TCP packets: 1. TCP subcontract whose header is smaller than *tcpfrag-value*; 2. TCP subcontract whose offset is 1. It can defend against TearDrop attack

The tcpsmurf sub-function can defend against tcpsmurf attack, preventing TCP messages whose destination address is the broadcast address

The icmpsmurf sub-function can defend against icmpsmurf attack, preventing ICMP messages whose destination address is the broadcast address

The ipsmurf sub-function can defend against ipsmurf attack, preventing IP messages whose destination address is the broadcast address

Example

The following example shows how to set DoS attack prevention subfunctions in global mode to prevent IP messages whose source IP address is same as destination IP address

Switch_config#dos enable ip

The following example shows how to set **dos enable tcpflags** to check illegal TCPflag messages in global mode.

Switch_config#dos enable tcpflags

12.2 show dos

Syntax

show dos

It is used to show all DoS attack prevention functions that users have set

Parameter

None

Default value

None

Remarks

EXEC mode

Example

The following example shows how to display all DoS attack prevention functions

Switch_config#dos enable all

Switch_config#show dos

dos enable icmp

dos enable ip

dos enable l4port

dos enable mac

dos enable tcpflags

dos enable tcpfrag

dos enable tcpsmurf

dos enable icmpsmurf

dos enable ipsmurf

Switch_config#

The following example shows how to set **dos enable ip** to display the sub-function that users have set

Switch_config#dos enable ip

Switch_config#show dos

dos enable ip

Chapter 13 EAPS Configuration Commands

13.1 Global Configuration Commands

13.1.1 ether-ring

Syntax

To set an instance of ring and enter the node mode, run the following command:

ether-ring *id*

To cancel an instance of ring, run the following command:

no ether-ring *id*

Parameter

Parameter	Description
id	ID of the node instance, range 0-32

Default

By default, the ring node is not configured

Command Mode

Global configuration mode

Usage Guidelines

STP should not be disabled before the configuration of node instance

Example

```
S1_config#ether-ring 1
S1_config_ring1#
```

Related Command

None

13.1.2 control-vlan

Syntax

To set the control VLAN of the ring node, run the following command:

control-vlan *vlan-id*

Parameter

Parameter	Description
vlan-id	ID of the control VLAN Value range: 1-4094

Default

By default, the control VLAN of a node is not configured

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. Any VLAN can be configured as the control VLAN of the node. When specifying the control VLAN, the corresponding VLAN system will be created. In this case, the user does not need to manually create the system VLAN

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the Ethernet ring has already been started

Example

S1_config#ether-ring 1
S1_config_ring1#control-vlan 2

Related Command

ether-ring

master-node

transit-node

13.1.3 master-node

Syntax

To configure an Ethernet ring as a master node, run the following command:

master-node

Parameter

None

Default

By default, the node type is not configured

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node or a transit node

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started

Example

S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node

Related Commands

control-vlan

transit-node

13.1.4 transit-node

Syntax

Configures the node type to be a transit node

transit-node

Parameter

None

Default

By default, the node type is not configured

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node or a transit node

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started

Example

S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#transit-node

Related Commands

control-vlan

master-node

13.1.5 hello-time

Syntax

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

hello-time *value*

To resume the Default of the cycle, run the following command:

no hello-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second The Default is one second. The value ranges between 1 and 10 seconds

Default

By default, the hello-time is one second

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The hello-time configuration validates only on the master node

2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked.

Example

S1_config#ether-ring 1

S1_config_ring1#control-vlan 2

S1_config_ring1#master-node

S1_config_ring1#hello-time 2

Related Command

fail-time

13.1.6 fail-time

Syntax

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

fail-time *value*

To resume the Default of the fail-time, run the following command:

no fail-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second The Default is three seconds. The value ranges between 3 and 30 seconds

Default

By default, the fail-time is 3 seconds

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The fail-time configuration validates only on the master node

2. By default, the value of the fail-time is triple of the fail-time, which avoids the Ethernet ring protocol from being shocked. After modifying the hello-time, you need to adjust the fail-time accordingly

Example

S1_config#ether-ring 1

S1_config_ring1#control-vlan 2

S1_config_ring1#master-node

S1_config_ring1#hello-time 2

S1_config_ring1#fail-time 6

Related Command

hello-time

13.1.7 pre-forward-time

Syntax

Configures the time of maintaining the pre-forward state on the transit port

pre-forward-time *value*

To resume the Default of the pre-forward-time, run the following command:

no pre-forward-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second The Default is three seconds. The value ranges between 3 and 30 seconds

Default

By default, the pre-forward-time is 3 seconds

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The pre-forward-time configuration validates only on the transit node

2. By default, the pre-forward-time on the transit node is three times the value of the hello-time on the master node, which avoids the network loop from being occurred after the transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node need be adjusted

Example

S1_config#ether-ring 1

S1_config_ring1#control-vlan 2

S1_config_ring1#transit-node

S1_config_ring1#pre-forward-time 8

Related Command

None

13.2 Port Configuration Commands

13.2.1 ether-ring primary-port

Syntax

To set a port to be the primary port of a master node, run the following command:

ether-ring *id* **primary-port**

To cancel the primary port configuration of a port, run the following command:

no ether-ring *id* **primary-port**

Parameter

Parameter	Description
id	ID of the node instance

Default

The primary port is not configured by default

Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port

Usage Guidelines

The primary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type is the master node

Example

S1_config#interface GigaEthernet 0/1

S1_config_g0/1#ether-ring 1 primary-port

S1_config_g0/1#exit

Related Command

master-node

ether-ring secondary-port

13.2.2 ether-ring secondary-port

Syntax

To set a port to be the secondary port of a master node, run the following command:

ether-ring *id* **secondary-port**

To cancel the secondary port configuration, run the following command:

no ether-ring *id* **secondary-port**

Parameter

Parameter	Description
id	ID of the node instance

Default

The secondary port on the master node is not configured by default

Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port

Usage Guidelines

The secondary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type must be the master node

Example

S1_config#interface GigaEthernet 0/3

S1_config_g0/3#ether-ring 1 secondary-port

S1_config_g0/3#exit

Related Command

master-node

ether-ring primary-port

13.2.3 ether-ring transit-port

Syntax

To set a port to be the transit port of a transit node, run the following command:

ether-ring *id* **transit-port**

To cancel the transit port, run the following command:

no ether-ring *id* **transit-port**

Parameter

Parameter	Description
id	ID of the node instance

Default

The transit port on the transit node is not configured by default

Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port

Usage Guidelines

The transit port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type must be the transit node. Two transit ports can be configured on one transit node

Example

S1_config_ring1#exit

S1_config#interface GigaEthernet 0/1

S1_config_g0/1#ether-ring 1 transit-port

S1_config_g0/1#exit

S1_config#interface GigaEthernet 0/3

S1_config_g0/3#ether-ring 1 transit-port

S1_config_g0/3#exit

Related Command

transit-node

13.3 Show Configuration Commands

13.3.1 show ether-ring

Syntax

To display the summary information about the Ethernet-ring node, run the following command:

show ether-ring *id*

To display the detailed information about the Ethernet-ring node, run the following command:

show ether-ring *id* **detail**

To display the information about the Ethernet-ring port, run the following command:

show ether-ring *id* **interface** *intf-name*

To display the summary information about the Ethernet-ring node, run the following command:

show ether-ring <cr>

Parameter

Parameter	Description
id	ID of the node instance
intf-name	Name of an interface

Default

None

Command Mode

EXEC, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

None

Related Command

None

Chapter 14 ERPS Configuration Commands

14.1 Global Configuration Commands

14.1.1 Erps

Syntax

To set an instance of ring and enter the node mode, run the following command:

erps *id*

To cancel an instance of ring, run the following command:

no erps *id*

Parameter

Parameter	Description
id	ID of the node

Default

By default, the ring node is not configured

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

Switch_config# erps 1

Switch_config_ring1#

Related Command

None

14.1.2 erps nimble-mode

Syntax

To configure erps nimble mode, use the following command

Parameter

None

Default

Disable

Command mode

Global Configuration Mode

Usage Guidelines

Before co**erps nimble-mode**

To remove erps nimble mode, use the no form of the command

no erps nimble-mode

nfiguring erps nimble mode, disable the spanning tree protocol

Example

Switch_config# **erps nimble-mode**

Related comamnd

None

14.1.3 control-vlan

Syntax

To set the control vlan value of the local node, run the following command:

control-vlan *value*

To return to the default setting, use the no form of this command.

no control-vlan

Parameter

Parameter	Description
value	The value ranges from 1 to 4094

Default

No control-vlan

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

The command is the compulsory option for the node configuration. The node cannot be modified after it works well

Example

Switch_config# erps 1

Switch_config_ring1#

Switch_config_ring1# control-vlan 2

Related Command

None

14.1.4 interconnection-node

Syntax

To configure the local node as the interconnection node, run the following command:

interconnection-node

To configure the local node as the non-interconnection node, run the following command:

no interconnection-node

Parameter

None

Default

The local node is the non-interconnection node.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

The command is the compulsory option for the node configuration. The node cannot be modified after it works well. Though the command is a compulsory option, it has a default configuration. So if you don't need to modify the default value, skip the step

Example

Switch_config# erps 1

Switch_config_ring1#

Switch_config_ring1# interconnection-node

Related Command

None

14.1.5 raps-virtual-channel

Syntax

To configure the local node, run R-APS virtual channel

raps-virtual-channel

To return to the default setting, use the no form of this command

no raps-virtual-channel

Parameter

None

Default

R-APS virtual channel

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

The command is the compulsory option for the node configuration. The node cannot be modified after it works well. Though the command is a compulsory option, it has a default configuration. So if you don't need to modify the default value, skip the step

Example

Switch_config# erps 1

Switch_config_ring1#

Switch_config_ring1# raps-virtual-channel

Related Command

None

14.1.6 revertive-mode

Syntax

To configure the revertive mode of the local node as the revertive mode, run the following command:

revertive-mode

To return to the default setting, use the no form of this command

no revertive-mode

Parameter

None

Default

revertive-mode

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

The command is the compulsory option for the node configuration. The node cannot be modified after it works well. Though the command is a compulsory option, it has a default configuration. So if you don't need to modify the default value, skip the step

Example

Switch_config# erps 1

Switch_config_ring1#

Switch_config_ring1#revertive-mode

Related Command

None

14.1.7 version

Syntax

To configure the version of the local node, run the following command:

version *value*

To return to the default setting, use the no form of this command.

no version

Parameter

Parameter	Description
value	The default value is 1. The value ranges from 0 to 2

Default

1

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

Switch_config# erps 1

Switch_config_ring1#

Switch_config_ring1# version 1

Related Command

None

14.1.8 wtr-time

Syntax

To configure the timeout time of the WTR timer, run the following command:

wtr-time *value*

no wtr-time

Parameter

Parameter	Description
value	The timeout time of WTR is 20s by default. The value ranges from 10 to 720s

Default

The timeout time of WTR is 20s by default

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

Switch_config# erps 1

Switch_config_ring1#

Switch_config_ring1# wtr-time 15

Related Command

None

14.1.9 guard-time

Syntax

To configure the timeout time of the Guard timer, run the following command:

guard-time *value*

no guard-time

Parameter

Parameter	Description
value	The timeout time of the Guard timer. Unit: 1ms. The default is 500. The value ranges from 10 to 2000. The step is 10ms

Default

The timeout time of the Guard timer is 500 milliseconds by default

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

When a port is recovered from an invalid state, the Guard timer is forbidden to handle the received protocol packets to avoid outdated packets from generating inaccurate protocols

Example

Switch_config# erps 1

Switch_config_ring1# guard-time 60

Related Command

None

14.1.10 send-time

Syntax

To set the interval of transmission of the protocol packets, run the following command:

send-time *value*

no send-time

Parameter

Parameter	Description
value	The timeout time of the timer. The default value is 5 seconds. The value ranges from 1 to 10 seconds

Default

By default, ERPS PDU is transmitted every five seconds

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

Switch_config_ring1# wtr-time 15

Switch_config_ring1# send-time 5

Related Command

None

14.2 Port Configuration Commands

14.2.1 erps ring-port

Syntax

To set a port to be a common ring port, run the following command:

erps *id* **ring-port**

To delete the common ring port or the ring configuration on the RPL port, run the following command:

no erps *id* **ring-port**

Parameter

Parameter	Description
id	ID of the node

Default

None

Command Mode

Configuration mode of the switching port (physical port or aggregation port)

Usage Guidelines

ERPS can set a physical or aggregation port to be a ring port. However, the physical port where link aggregation, 802.1X or port security has been configured can not be set to be an ERPS ring port

The default VLAN for each ring port must be configured to be consistent so that ERPS packets can be normally forwarded

Example

Switch_config# interface f0/1

Switch_config_f0/1# erps 1 ring-port

Related Command

None

14.2.2 erps rpl

Syntax

To set a port to be a RPL (ring protection link) port of ERPS, run the following command:

erps *id* **rpl**

To delete the RPL port and retain its role as a common ring port, run the following command:

no erps *id* **rpl**

Parameter

Parameter	Description
id	ID of the node

Default

None

Command Mode

Configuration mode of the switching port (physical port or aggregation port)

Usage Guidelines

In case of automatic discovery, the function of the erps rpl command is as same as the priority value is modified to 0

If you want to delete the ring settings of the port, run the following command

no erps *id* **ring-port**

Example

Switch_config_f0/1# interface f0/3
Switch_config_f0/3# erps 1 rpl

Related Command

None

14.2.3 erps neighbor

Syntax

To set the port as ERPS RPL neighbor, run the following command

erps *id* **neighbour**

To return to the default setting, use the no form of this command

no erps *id* **neighbour**

Parameter

Parameter	Description

id	ID of the node

Default

None

Command Mode

Configuration mode of the switching port (physical port or aggregation port)

Usage Guidelines

Set a port to be RPL of a designated node. Meanwhile, the port must be connected to the RPL port and become the RPL neighbor port

Example

Switch_config_f0/1# interface f0/3

Switch_config_f0/3# erps 1 neighbour

Related Command

None

14.2.4 erps mep

Syntax

To bind ERPS port and MEP port, run the following command:

erps *id* **mep [up | down] md** *md-WORD* **ma** *ma-WORD* **level** *level-id* **local** *local-id* **remote** *remote-id*

To return to the default setting, use the no form of this command

no erps *id* **mep [up | down]**

Parameter

Parameter	Description
id	ID of Ethernet ring
md-WORD	MEP maintenance domain information
ma-WORD	MEP maintenance link information
level-id	MEP level information
local-id	MEP local id information

remote-id	MEP remote id information

Default

None

Command Mode

Configuration mode of the switching port (physical port or aggregation port)

Usage Guidelines

The command is used to configure CFM port, then bind ERPS port and MEP port

Example

Switch_config_f0/1# interface f0/3

Switch_config_f0/3# erps 1 mep down md d ma d level 4 local 4 remote 1

Related Command

None

14.3 Control Commands

14.3.1 erps [ForcedSwitch | ManualSwitch | Clear]

Syntax

To force the node switch to the interface *interface-type interface-number*, run the following command:

erps *id* **ForcedSwitch interface** *interface-type interface-number*

To force the node switch to the interface *interface-type interface-number* manually, run the following command:

erps *id* **ManualSwitch interface** *interface-type interface-number*

To clear the switch command of the node, run the following command:

erps *id* **Clear**

Parameter

Parameter	Description
id	ID of the node
interface-type	Type of the interface

interface-number	Number of the interface

Default

None

Command Mode

Monitoring mode

Usage Guidelines

None

Example

None

Related Command

None

14.4 Show Configuration Commands

14.4.1 show erps

Syntax

To show the abstract information of the ERPS, run the following command:

show erps [*id*]

To show the detailed information of the Ethernet ring node, run the following command:

show erps *id* **detail**

To show the information of the Ethernet interface, run the following command:

show erps interface *intf-name*

Parameter

Parameter	Description
id	ID of the node
intf-name	Interface name

Default

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

None

Related Command

None

Chapter 15 GVRP Configuration Commands

15.1 GVRP Configuration Commands

15.1.1 GVRP

Syntax

To enable GVRP globally on a device and on an interface, use the **gvrp** command. To disable GRVP, use the no form of this command

gvrp

no gvrp

Parameter

None

Default

GVRP is disabled globally

GRVP is enabled on each interface

Usage Guidelines

GVPRP can be enabled globally or on an interface in the system, and GVRP is not enabled until both of them are enabled

Example

The following example configures global gvrp on the device and interfaces:

Switch_config#gvrp

Switch_config#

The following example enables gvrp on interface 1:

Switch_config_g0/1#gvrp

Switch_config_g0/1#

15.1.2 gvrp dynamic-vlan-pruning

Syntax

gvrp dynamic-vlan-pruning

no gvrp dynamic-vlan-pruning

To set the dynamic VLAN only takes effect on the registered interface, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

None

Default

Dynamic-vlan-prunning is disabled. That is, dynamic VLAN can take effect in all interfaces

Command Mode

Global configuration mode

Usage Guidelines

After this command is enabled and, if a port has not registered a dynamic VLAN, this port will not belong to the dynamic VLAN even though this port is a trunk port and it allows the dynamic VLAN to pass through

Example

The following example shows how to make dynamic VLAN validate on its registered port

Switch_config#gvrp dynamic-vlan-pruning

Switch_config#

15.1.3 Show gvrp statistics

Syntax

To show gvrp statistics, use the show gvrp statistics command

show gvrp statistics [interface *intf-id*]

Parameter

Parameter	Description
intf-id	The concrete physical interface

Default

None

Usage Guidelines

Show GVRP statistics

Example

The following example show GVRP statistics of port g0/1:

Switch_config#show gvrp statistics interface g0/1

GVRP statistics on port g0/1

GVRP Status : Enabled

GVRP Frames Received : 0

GVRP Frames Transmitted : 20

GVRP Frames Discarded : 0

GVRP Last Pdu Origin : 0000.0000.0000

15.1.4 Show gvrp status

Syntax

To show GVRP status information, use **show gvrp status** command

show gvrp status

Parameter

None

Default

None

Usage Guidelines

Show GVRP status information

Example

The following command shows GVRP status information of the switch:

Switch_config#show gvrp status

GVRP is enabled

15.1.5 Debug gvrp event

Syntax

To enable debugging GVRP event information, use the **debug gvrp event** command. Use the no form of this command to disable debugging

debug gvrp event

no debug gvrp event

Parameter

None

Default

None

Usage Guidelines

Enable/disable debugging GVRP event information

Example

Switch# debug gvrp event

Switch#

15.1.6 Debug gvrp packet

Syntax

To enable debugging GVRP packet information, use the **debug gvrp event** command. Use the no form of this command to disable debugging

debug gvrp packet

no debug gvrp packet

Parameter

None

Default

None

Usage Guidelines

Enable/disable debugging GVRP packet information

Example

switch# debug gvrp packet

switch#

15.2 GARP Configuration Commands

GARP is the basic module of GVRP/GMRP. It is intended to scheduler GVRP/GMRP operation and provide services

15.2.1 Garp timer leaveall

Syntax

To configure garp leaveall timer, use the **garp timer leaveall** command. Use the no form of this command to restore the default value.

garp timer leaveall *time_value*

no garp timer leaveall

Parameter

Parameter	Description
timer_value	Global leaveall timer value. Value range: 10–32765 centseconds.

Default

1000 centiseconds

Usage Guidelines

Bridge will clear all registered VLAN information and send out LeaveAll Message after leaveall timer expires

Example

The following example configures leaveall timer on the switch to 1200 centiseconds:

Switch_config# garp timer leaveall 1200

Switch_config#

15.2.2 garp timer hold

Syntax

garp timer hold time_value

no garp timer hold

To set grap hold timer, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
timer_value	The hold timer value of the interface. The value ranges from 10 to 32765 centiseconds

Default

10 centiseconds

Command Mode

Interface configuration mode

Usage Guidelines

None

Example

The following example shows how to set the garp hold timer on the interface g0/1 to 15 centiseconds

Switch_config_g0/1#garp timer hold 15

Switch_config_g0/1#

15.2.3 garp timer join

Syntax

garp timer join time_value

no garp timer join

To set garp join timer, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
timer_value	The join timer value of the interface. The value ranges from 10 to 32765 centiseconds

Default

20 centiseconds

Command Mode

Interface configuration mode

Usage Guidelines

None

Example

The following example shows how to set garp join timer on interface g0/1 to 25 centiseconds.

Switch_config_g0/1#garp timer join 25

Switch_config_g0/1#

15.2.4 garp timer leave

Syntax

garp timer leave time_value

no garp timer leave

To set garp leaver timer, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
timer_value	The leave timer value of the interface. The value ranges from 10 to 32765 centiseconds

Default

60 centiseconds

Command Mode

Interface Configuration Mode

Usage Guidelines

None

Example

The following example shows how to set the value of the garp leave timer on interface g0/1 to 80 centiseconds

Switch_config_g0/1#garp timer leave 80

Switch_config_g0/1#

15.2.5 show garp timers

Syntax

show garp timers [interface *intf_id*]

To show the GARP-configured clock information, run the above command

Parameter

Parameter	Description

intf-id	The concrete physical port

Default

None

Usage Guidelines

This command is used to display the GARP-configured clock information, including the global leaveall timer value, the hold/join/leave timer value on the port

Example

The following example shows how to show the timer configuration information on interface G0/1

Switch# show garp timers interface g0/1

GARP timers on port 1(G0/1)

Garp Join Time : 20 centiseconds

Garp Leave Time : 60 centiseconds

Garp LeaveAll Time : 1000 centiseconds

Garp Hold Time : 10 centiseconds

15.2.6 Show garp status

Syntax

To show the currently-running garp application example, use the **show garp status** command

show garp status

Parameter

None

Default

None

Usage Guidelines

Display the currently running GARP statistics

Example

The following example shows the currently running GARP statistics:

Switch_config#show garp status

No GARP application is running

15.2.7 Debug garp

Syntax

To enable the garp event or timer debuging information, use the debug garp event command. Use the no form of this command to disable debugging

debug garp { event | timer }

no debug garp { event | timer }

Parameter

Parameter	Parameter description
event	Event debug
timer	Timer debug

Default

None

Usage Guidelines

Use this command to enable/disable debugging GARP event information

Example

The following example shows how to enable debugging GARP event information

Switch# debug garp event

Switch#

Chapter 16 IGMP Proxy Commands

16.1 ip igmp-proxy enable

Syntax

ip igmp-proxy enable

no ip igmp-proxy enable

To enable or disable igmp-proxy, run **ip igmp-proxy enable**. To resume the default value, run **no ip igmp-proxy enable**. Note that the igmp-proxy function is predicated on igmp-snooping, so you must first enable igmp-snooping before configuring this command

Parameter

None

Default value

The IGMP proxy is disabled by default

Usage guidelines

None

Example

The following example shows how to enable the igmp-proxy:

switch_config# ip igmp-snooping

switch_config# ip igmp-proxy enable

switch_config#

16.2 ip igmp-proxy agent-vlan client-vlan map

Syntax

ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*

no ip igmp-proxy agent-vlan avlan_map **client-vlan map** cvlan_map

Parameter

Parameter	Description
avlan_map	Agent VLAN
cvlan_map	Customer VLAN

Default value

None

Usage guidelines

1. The represented VLAN cannot be configured before vlan is designated by avlan_map; also, the agent VLAN cannot be configured before cvlan_map

2. The represented and agent VLANs must accept the control of igmp-snooping

Example

The following example shows how to set vlan2 to be the agent vlan of vlan1

switch_config# ip igmp-proxy agent-vlan 2 client-vlan map 1

switch_config#

16.3 show ip igmp-proxy

Syntax

show ip igmp-proxy

Parameter

None

Default value

None

Usage guidelines

This command is used to display the configurations about IGMP proxy

Example

The following example shows how to display the configurations of IGMP proxy.

switch#show ip igmp-proxy

Global IGMP proxy configuration:

Globally enable: Enable

Agent: vlan 2, it has been alloced

Client static : vlan 1

Client auto : vlan

Agent: vlan 3, it has been alloced

Client static : vlan 1

Client auto : vlan

Globally clients list

Client : vlan 1, it has been alloced

Static Multi-source list

Static Source : No Static Source

switch#

16.4 debug ip igmp-proxy

Syntax

debug ip igmp-proxy *[error | event | packet]*

no debug ip igmp-proxy *[error | event | packet]*

Parameter

Parameter	Description
event	Debugs the igmp-snooping event
packet	Debugs the reception and transmission of igmp-snooping
error	Debugs the igmp-snooping errors

Default value

None

Usage guidelines

This command is used to enable or disable the debugging & printing switch of IGMP-proxy

Chapter 17 IGMP-SNOOPING Configuration Commands

17.1 igmp-snooping

Syntax

To enable the IGMP-snooping of VLAN, use the ip igmp-snooping command. Use the no form of this command to restore the default.

ip igmp-snooping [vlan *vlan_id* **]**

no ip igmp-snooping [vlan *vlan_id* **]**

Parameter

Parameter	Description
vlan id	VLAN identity.Value is from 1 to 4094

Default

Disabled

Usage Guidelines

If not specified the vlan parameter, this command enable or disable all vlans in the system (IGMP-snooping currently can be ran on 16 vlans at most at the same time.)

Example

The following command enables IGMP snooping of vlan 1:

switch(config)# ip igmp-snooping vlan 1

switch(config)#

17.2 igmp-snooping static

Syntax

ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*

no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*

Parameter

Parameter	Description

vlan id	VLAN identity.Value is from 1 to 4094
A.B.C.D	Specifies the IP address of multicast
inft	Specifies the interface

Default

None

Usage Guidelines

Use this command to configurethe the static multicast address of vlan. Use the no form of this command to delete the address

Example

The following command adds the static multicast address at 234.5.6.7 to the fast ethernet interface G0/5 of vlan 2:

switch_config# ip igmp-snooping vlan 2 static 234.5.6.7 interface gigaEthernet0/5

switch_config#

Note:

224.0.0.0-224.0.0.255, as the multicast address which cannot be routed, cannot be registered to each interface

17.3 igmp-snooping immediate-leave

Syntax

In global configuration mode:

To configure the immediate-leave characteristic of vlan, use the **ip igmp-snooping vlan** command. Use the no form of this command to restore the default

ip igmp-snooping vlan *vlan_id* **immediate-leave**

no ip igmp-snooping vlan *vlan_id* **immediate-leave**

Parameter

Parameter	Description
vlan id	VLAN identity. Value is from 1 to 4094

Default

Disabled

Syntax

In interface configuration mode:

To configure the immediate-leave characteristic of vlan, use the **ip igmp-snooping immediate-leave** command.Use the no form of this command to restore the default

ip igmp-snooping immediate-leave

no ip igmp-snooping immediate-leave

Parameter

None

Default

Disabled

Usage Guidelines

Configuring the immediate-leave feature of a VLAN or port allows the switch to delete the port from the port list of the corresponding multicast group immediately after receiving the leave message on the port, instead of turning on the timer and waiting for other hosts to join this multicast. If other hosts under the same port also belong to this group but do not want to leave, the multicast communication of these users may be affected, and the immediate-leave function should not be enabled at this time

The immediate-leave configuration of the port and the immediate-leave configuration of the VLAN work simultaneously

Example

The following command enables immediate-leave characteristic of vlan 1:

switch_config# ip igmp-snooping vlan 1 immediate-leave
switch_config#

The following command enables immediate-leave characteristic of interface g0/8:

switch_config_g0/8#ip igmp-snooping immediate-leave

17.4 igmp-snooping mrouter

Syntax

ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*

no ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*

Parameter

Parameter	Description
vlan id	VLAN identifier. The value ranges from 1 to 4094
intf	Interface

Default

None

Usage Guidelines

The command is used to configure the static route port. Use the no form of this command to delete the route port

Only static routing ports can be configured for existing VLANs

Example

The following example shows how to add the gigabit Ethernet G0/5 of VLAN 2 as its static route port

switch_config# ip igmp-snooping vlan 2 mrouter interface GigaEthernet0/5

switch_config#

17.5 igmp-snooping policy

Syntax

ip igmp-snooping policy *word*

no ip igmp-snooping policy

Parameter

Parameter	Description
Word	IP ACL name

Default

None

Usage Guidelines

The command is used to configure the IP ACL list when igmp-snooping adds the multicast forwarding table. To return to the default setting, use the no form of this command. Ipacl must already exist when configuring this command

Example

The following example shows how to detect the IP ACI named 123 when adding the multicast forwarding table

switch_config# ip igmp-snooping policy 123

switch_config#

17.6 igmp-snooping dlf-drop

Syntax

ip igmp-snooping dlf-drop

no ip igmp-snooping dlf-drop

Default

Parameter	Description
	Filter unregistered address multicast packets

Usage Guidelines

This command is used to set the multicast packets whose destination multicast addresses are not registered to the filtration mode. The negative form of this command is used to resume the default settings

Example

The following example shows how to drop the multicast packets with unregistered destination addresses in all VLANs.

switch_config# ip igmp-snooping dlf-drop

switch_config#

17.7 igmp-snooping router age

Syntax

ip igmp-snooping timer router-age *timer_value*

no ip igmp-snooping timer router-age

Parameter

Parameter	Description
time value	Query timer time. Value is from 10 to 2147483647

Default

260 seconds

Usage Guidelines

Use this command to configure query timer time. Use the no form of this command to restore the default value

Example

The following example configures router-age to 300 seconds

switch(config)# ip igmp-snooping timer router-age 300

switch(config)#

17.8 igmp-snooping response time

Syntax

To configure the maximum response time of IGMP-snooping, use IGMP-snooping command. Use the no form of this command to restore the default value

ip igmp-snooping timer response-time *timer_value*

no ip igmp-snooping timer response-time

Parameter

Parameter	Description
time value	Query timer time. The value ranges from 1 to 2147483647

Default

15 seconds

Usage Guidelines

None

Example

The following example configures response-time to 20 seconds:

switch(config)# ip igmp-snooping timer response-time 20

switch(config)#

17.9 igmp-snooping querier

Syntax

To activate IGMP-snooping querier mechanism or configure the source ip address of the spontaneous query packets. Use the no form of this command to restore the default value

ip igmp-snooping querier [address *<ip_addr>***]**

no ip igmp-snooping querier [address *<ip_addr>***]**

Parameter

Parameter	Description
ip_addr	Tthe common unicast IP address

Default

Disabled,the default source IP address is 10.0.0.200

Usage Guidelines

None

Example

The following command activates IGMP quirier:

switch(config)# ip igmp-snooping querier

switch(config)#

17.10 igmp-snooping querier querier-timer

Syntax

ip igmp-snooping querier querier-timer *time_value*

no ip igmp-snooping querier querier-timer

To configure the forward interval of forwarding query packets by the local querier, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
time_value	The query interval of the local querier

Default

The default interval is 200s when enable the Querier function

Usage Guidelines

None

Example

The following command shows how to configure the query period of the local querier as 140s.

switch_config# ip igmp-snooping querier querier-timer 140

switch_config#

17.11 igmp-snooping forward-l3-to-mrouter

Syntax

ip igmp-snooping forward-l3-to-mrouter

no ip igmp-snooping forward-l3-to-mrouter

To send the data packets to the multicast routing port, run **ip igmp-snooping forward-l3-to-mrouter**. To return to the default setting, use the no form of this command

Parameter

None

Default

If the forward-l3-to-mrouter command is not enabled, the data packets will not be sent to the related multicast routing port

Usage Guidelines

This command is mainly to send the data packets to the IGMP JOIN port and meanwhile to the multicast routing port. Especially in case of L3 multicast cascading, the upstream L3 switches cannot receive the IGMP JOIN packets from a relative group and hence cannot learn the information about the relative group, and then the data packets will be sent to all physical ports in the L3 egress VLAN. After this command is run, the data packets will only be sent to the multicast routing port, which is registered on PIM-SM

Example

The following example shows how to activate IGMP forward-l3-to-mrouter and make the upstream multicast data packets be sent to the multicast routing port:

switch_config# ip igmp-snooping forward-l3-to-mrouter

switch_config#

17.12 igmp-snooping sensitive

Syntax

ip igmp-snooping sensitive [value *int<3-30>***]**

no ip igmp-snooping sensitive [value]

To activate IGMP-snooping sensitive mechanism or set the value of sensitive, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
int	3-30, unit: second

Default

The sensitive function is disabled. The default valueis 5s

Usage Guidelines

This command is mainly used to modify the router-age of the mrouter port in active state and deliver the new query packets rapidly when a port in trunk mode is shut down

Example

The following example shows how to activate IGMP sensitive and set the route-age of mrouter to be a converged one

switch_config# ip igmp-snooping sensitive

switch_config# ip igmp-snooping sensitive value 10

17.13 igmp-snooping v3-leave-check

Syntax

ip igmp-snooping v3-leave-check

no ip igmp-snooping v3-leave-check

To send the special query packets after the v3-leave packet is received, run ip igmp-snooping v3-leave-check; To return to the default setting, use the no form of this command

Default

v3-leave-check is disabled and the special query packet will not be sent after v3-leave packet is received

Parameter

None

Usage Guidelines

None

Example

The following example shows how to activate IGMP v3-leave-check and send the special query packet after the v3-leave packet is received

switch_config# ip igmp-snooping v3-leave-check

switch_config#

17.14 igmp-snooping forward-wrongiif-within-vlan

Syntax

ip igmp-snooping forward-wrongiif-within-vlan

no ip igmp-snooping forward-wrongiif-within-vlan

To send the multicast data packets, received from the wrongiif port, to the relative physical ports in the local vlan, run ip igmp-snooping forward-wrongiif-within-vlan; To return to the default setting, use the no form of this command

Parameter

None

Default

This command is enabled by default and the multicast packets from the wrongiif port will be sent to the relative physical ports

Usage Guidelines

This comman takes its importance only when the L3 multicast is enabled. After this command is enabled, the multicast packets, entering from the wrongiif port, will be sent to the physical ports that are added into the group of vlan; otherwise, the multicast packets will be dropped

Example

The following example shows how to activate IGMP forward-wrongiif-within-vlan, and how to send the multicast packets from the wrongiif port to the relative physical ports in the local VLAN:

switch_config# ip igmp-snooping forward-wrongiif-within-vlan

switch_config#

17.15 igmp-snooping filter

Syntax

ip igmp-snooping filter *word*

no ip igmp-snooping filter

Parameter

Parameter	Description
word	IP ACL name

Default

None

Usage Guidelines

If the IPACL function of IGMP-snooping port is enabled, the IPACL will be used under the port to specify the packets of a multicast IP address to be processed or ignored

Command Mode

Interface configuration mode

Example

The following example shows how to configure IP ACL deny-pc on port g0/2:

switch_config#ip access-list standard deny-pc

switch_config_std#deny 239.255.255.250 255.255.255.255

switch_config_std#permit any

switch_config_std#exit

switch_config#interface g0/2

switch_config_g0/2#ip igmp-snooping filter deny-pc

17.16 igmp-snooping vlan filter

Syntax

ip igmp-snooping vlan *vlanid-list* **filter** *ipaddr-list*

no ip igmp-snooping vlan *vlanid-list* **filter** *ipaddr-list*

Parameter

Parameter	Description
Vlanid-list	VLAN ID list, connect with "," and "-". Range from 1 to 4094
ipaddr-list	Multicast IP address list, connect with "," and "-" ("," and "-" must be followed by at least 1 space)

Default

None

Usage Guidelines

If multicast filtering in the IGMP-snooping VLAN is enabled, only the multicast group report request in the

filtering list will be accepted and added to the group in the VLAN, otherwise it will be discarded and no group will be added

Command Mode

Global configuration mode

Example

The following example shows how to configure filter list on VLAN 2:

switch_config#ip igmp-snooping vlan 2 filter 230.1.1.1 - 230.1.1.100

17.17 igmp-snooping limit

Syntax

ip igmp-snooping limit *value*

no ip igmp-snooping limit

Parameter

Parameter	Description
value	1-2048

Default

2048

Usage Guidelines

The command configures the max multicast IP address number in the port of IGMP-snooping. The command will estimate whether the applied groups have reached the configuration number when IGMP-snooping generating the forward table. Otherwise, the table of the port is no longer generated

Command Mode

Interface configuration mode

Example

The following example shows how to set the max number of the joining group as 1000.

switch_config_G0/1# ip igmp-snooping limit 1000

switch_config_G0/1#

17.18 igmp-snooping report-suppression

Syntax

ip igmp-snooping report-suppression [**max-number** *value*]

no ip igmp-snooping report-suppression

Parameter

Parameter	Description
value	This parameter specifies the maximum number of reports that can be forwarded to the same multicast group in a query period within the same VLAN after report-suppression is enabled. The value ranges from 1 to 5. If this command is configured without keyword max-number, the maximum number of report forwarding is 1

Default

Disabled

Usage Guidelines

If the report-suppression function of IGMP-snooping is configured, in the same VLAN, for the report request of a multicast group, whether the client enables the function in the initial state or the response to the query, the switch forwards only a limited number to the mrouter port. The forwarding number is determined by the Parameter after max-number, and the range is from 1 to 5. If the max-number keyword is omitted, the number of forwardings is 1 by default

This function is to reduce the processing cost of the local switch and the upstream switch and save the bandwidth for forwarding report packets when the IGMP Snooping function is normal

Command Mode

Global configuration mode

Example

The following example shows how to enable report-suppression function of IGMP-snooping

switch_config# ip igmp-snooping report-suppression

switch_config#

17.19 igmp-snooping proxy-leave

Syntax

ip igmp-snooping proxy-leave

no ip igmp-snooping proxy-leave

Parameter

None

Default

Disabled

Usage Guidelines

If the IGMP-snooping proxy-leave function is configured, in the same VLAN, the switch sends the leave message of the multicast group to the upstream device only after all members of a multicast group have truly left the group

This function is to reduce the processing cost of the local switch and the upstream switch and save the bandwidth for forwarding report packets when the IGMP Snooping function is normal

Command Mode

Global configuration mode

Example

The following example shows how to enable the proxy-leave function of IGMP-snooping.

switch_config# ip igmp-snooping proxy-leave

switch_config#

17.20 show ip igmp-snooping

Syntax

show ip igmp-snooping

Parameter

None

Default

None

Usage Guidelines

Use this command to show configuration information of IGMP-snooping

Example

The following example shows the vlan information of the running ipmp-snooping:

switch_config# show ip igmp-snooping

Global IGMP snooping configuration:

Globally enable : Enabled

VLAN nodes : 1,50,100,200,400,500

Dlf-frames filtering : Disabled

Sensitive : Disabled

Querier : Enabled

Querier address : 10.0.0.200

Querier interval : 140 s

Router age : 260 s

Response time : 15 s

vlan_id	Immediate-leave	Ports	Router Ports
1	Disabled	5-10	SWITCH(querier);
50	Disabled	1-4	SWITCH(querier);
100	Disabled	NULL	SWITCH(querier);G0/1(static);
200	Disabled	NULL	SWITCH(querier);
400	Disabled	NULL	SWITCH(querier);
500	Disabled	NULL	SWITCH(querier);

switch_config#

17.21 show ip igmp-snooping timer

Syntax

show ip igmp-snooping timer

Parameter

None

Default

None

Usage Guidelines

Use this command to show timer information of IGMP

Example

The following example shows timer information of igmp-snooping:

switch_config# show ip igmp-snooping timer

vlan 1 mrouter on port 3 : 251

switch_config#

17.22 show ip igmp-snooping groups

Syntax

show ip igmp-snooping groups

Parameter

None

Default

None

Usage Guidelines

Use this command to display multicast group information of IGMP-snooping

Example

The following example shows the multicast group information of igmp-snooping:

switch_config# show ip igmp-snooping group

The total number of groups 2

Vlan Group Type Port(s)

---- --------------- ---- ---

1 226.1.1.1 IGMP G0/1G0/3

1 225.1.1.16 IGMP G0/1G0/3

switch_config#

17.23 show ip igmp-snooping group interface

Syntax

show ip igmp-snooping group interface

Parameter

None

Default

None

Usage Guidelines

Displays the IGMP-snooping multicast group information added on the port

Example

The following example shows how to display the igmp-snooping multicast group information on port g0/4.

Switch#show ip igmp-snooping group interface g0/4

Number of joined groups: 1

Vlan	Group	Mode	Source Num
2	230.1.1.1	Exclude	0

Switch#

17.24 show ip igmp-snooping statistics

Syntax

show ip igmp-snooping statistics [message|packet|hardware|vlan *vlanid***]**

Parameter

Parameter	Description
vlanid	When the command is followed by the optional keyword VLAN, it specifys the vlan ID

Default

None

Usage Guidelines

Display IGMP-snooping statistics. The keywords messge, packet, hardware, VLAN are optional. With optional keywords, the message statistics, received packet statistics, hardware operation statistics, and sub-VLAN statistics of the IGMP-Snooping task are displayed separately. Without optional keywords, global messages, messages, and hardware operation statistics are displayed. When using a keyword VLAN, you need to specify Parametervlanid to display the statistics under the VLAN

Example

The following example shows igmp-snooping statistics:

Switch#show ip igmp-snooping statistics

IGMP Snooping Message Statistics

L2 main messages sent OK : 305

L2 main messages sent failed : 0

L2 packets received : 302

L2 packets sent : 302

L2 packets sent failed : 0

L2 link-status messages : 3

IGMP Snooping messages received: 313

IGMP packet messages received : 302

IGMP Snooping Packet Statistics

Received packets : 302

IGMP packets : 259

M-routing protocol packets : 0

Other packets : 43

Received IGMP general queries : 0

Received IGMPv2 specific queries : 0

Received IGMPv3 g specific queries : 0

Received IGMPv3 gs specific queries: 0

Received IGMPv1 reports : 0

Received IGMPv2 reports : 230

Received IGMP leaves : 0

Received IGMPv3 reports : 29

Flooded queries : 0

Forwarded and proxy-sent reports : 0

Forwarded and proxy-sent leaves : 0

IGMP Snooping Hardware Operation Statistics

Total : 9

Succeeded : 9

Failed : 0

Report/leave processing: 5

Response timer expiring: 4

Group creating/updating: 7

Group deleting : 2

17.25 show ip igmp-snooping vlan

Syntax

show ip igmp-snooping vlan *vlan-id*

Parameter	Description
vlan	1-4094

Parameter

Default

None

Usage Guidelines

Display VLAN information of IGMP-snooping

Example

The following example shows how to display the vlan information of igmp-snooping.

Switch_config#show ip igmp-snooping vlan

vlan_id Immediate-leave Ports Router Ports

---

1 Disabled 7-30

2 Disabled NULL

switch_config#

17.26 debug ip igmp-snooping packet

Syntax

debug ip igmp-snooping packet

no debug ip igmp-snooping packet

Parameter

None

Default

None

Usage Guidelines

Use this command to enable/disable the packet debugging switch of IGMP-snooping

Example

The followig command enables the packet debugging switch of igmp-snooping:

switch# debug ip igmp-snooping packet

switch#

17.27 debug ip igmp-snooping timer

Syntax

debug ip igmp-snooping timer

no debug ip igmp-snooping timer

Parameter

None

Default

None

Usage Guidelines

Use this command to enable/disable the timer debugging switch of IGMP-snooping

Example

The following example enables timer debugging switch of igmp-snooping:

switch# debug ip igmp-snooping timer

switch#

17.28 debug ip igmp-snooping event

Syntax

debug ip igmp-snooping event

no debug ip igmp-snooping event

Parameter

None

Default

None

Usage Guidelines

Use this command to enable/disable the event debugging switch of IGMP-snooping

Example

The following example enable event debugging switch of igmp-snooping:

Switch#debug ip igmp-snooping event

Switch#

17.29 debug ip igmp-snooping error

Syntax

debug ip igmp-snooping error

no debug ip igmp-snooping error

Parameter

None

Default

None

Usage Guidelines

Use this command to enable/disable the error debugging switch of IGMP-snooping

Example

The following example shows how to enable error debugging switch of igmp-snooping:

Switch#debug ip igmp-snooping error

Switch#

17.30 debug ip igmp-snooping

Syntax

debug ip igmp-snooping

no debug ip igmp-snooping

Parameter

None

Default

None

Usage Guidelines

Turn on/off all debugging switches of igmp-snnoping

Example

The following example shows how to turn on all debugging switches of igmp-snooping

```
Switch#debug ip igmp-snooping
  IGMP-snooping packet debugging is on
  IGMP-snooping timer debugging is on
  IGMP-snooping event debugging is on
  IGMP-snooping error debugging is on
Switch#
```

Chapter 18 Interface Configuration Commands

18.1 interface

Syntax

[no] interface *port*

To enter the interface configuration mode, run the above-mentioned command. If the logical port is inexistent, you have to create this port first and then enter the port mode. If the physical port is inexistent, the command will fail to be executed. The negative form of this command has different functions for the physical port and the logical port

The **no interface physical-port** command is used to resume the default settings of the physical port

The **no interface** ***logical-port*** command is used to delete the logical port

Parameter

Parameter	Description
Port	Stands for the existent physical or logical port

Default

The default mode is not the port mode

Usage Guidelines

When you execute this command in configuration mode, you have to enable this command to be in port configuration mode first. When the port command is configured, you shall use the **exit** command to exit from the port mode

Example

The following example shows how to enter the port mode of port g0/1

Switch_config#

Switch_config#interface gigaEthernet0/1

Switch_config_g0/1#exit

Switch_config#

18.2 description

Syntax

[no] description *line*

To set the description information of a port, run the above-mentioned command

Parameter

Parameter	Description
line	Stands for the character string of the description information, among which space may exist

Default

There is no description information by default

Usage Guidelines

This command is configured in port configuration mode

Example

The following example shows how to set the description information of port g0/1 to "up link"

Switch_config# interface gigaEthernet0/1

Switch_config_g0/1# description uplink

18.3 bandwidth

Syntax

[no] bandwidth *kilobps*

To set the bandwidth of an interface, ran the above-mentioned command

Parameter

Parameter	Description
kilobps	Means the bandwidth of port, which ranges from 1 to 10000000 kbps

Default

The default bandwidths of the 100M port, gigabit port and 10G port are 100000kbps, 1000000kbps and 10000000kbps respectively

Usage Guidelines

This command is configured in port configuration mode

Note:

The configured bandwidth does not mean the actual bandwidth of a port, but is used by some protocol (such

as spanning tree) to calculate the port cost

Example

The following example shows how to set port g0/1 to 10000000

Switch_config # interface gigaEthernet0/1

Switch_config_g0/1# bandwidth 10000000

18.4 delay

Syntax

[no] delay *tensofmicroseconds*

To set the delay of an interface, run the above-mentioned command

Parameter

Parameter	Description
tensofmicroseconds	Port delay. The value ranges from 1 to 10000000 (10 ms)

Default

The Default of the delay is 1

Usage Guidelines

This command is configured in port configuration mode

Example

The following example shows how to set the delay of an interface to 10

Switch_config_g0/1# delay 10

18.5 shutdown

Syntax

[no] shutdown

To close a port, run **shutdown**; to restart a port, run **no shutdown**

Parameter

None

Default

The physical port is in **enabled** status by default

Usage Guidelines

This command can be used in port mode to enable or disable a port

Example

The following example shows how to enable port g0/1

Switch_config_g0/1#

Switch_config_g0/1# no shutdown

Switch_config_g0/1#

18.6 show interface

Syntax

show interface *<port>*

To browse the state of an interface, run the above-mentioned command

Parameter

Parameter	Description
Port	Name of an interface If a specific port is not in the command, the system will show the statuses of all ports

Default

None

Usage Guidelines

This command can be used in EXEC mode and configuration modes to show the physical status and packet reception statistics of a port

Example

The following example shows the information about port g0/1:

Switch_config# show interface gigaEthernet 0/1

GigaEthernet0/1 is administratively down, line protocol is down

Hardware is Giga-Combo-FX, address is 00e0.0fe4.d083 (bia 00e0.0fe4.d083)

MTU 1500 bytes, BW 1000000 kbit, DLY 10 usec

Encapsulation ARPA

Auto-duplex, Auto-speed

flow-control off

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

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

Received 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 align, 0 FCS, 0 symbol

0 jabber, 0 oversize, 0 undersize

0 carriersense, 0 collision, 0 fragment

0 L3 packets, 0 discards, 0 Header errors

Transmited 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 sqettest, 0 deferred

0 single, 0 multiple, 0 excessive, 0 late

0 L3 forwards

18.7 show running-config interface

Syntax

show running-config interface *port*

To display the settings of a port, run the above-mentioned command

Parameter

Parameter	Description
Port	Stands for the existent port

Default

None

Usage Guidelines

This command can be executed in EXEC or configuration mode to browse the settings of a port

Example

The following example shows the settings of port g1/1:

```
Switch_config#show running-config interface g0/1
Building configuration...

Current configuration:
!
interface GigaEthernet0/1
 shutdown
 description uplink
 bandwidth 10000000
 delay 10
Switch_config#
```

18.8 show cable interface

Syntax

show cable interface *port*

To display the the port cable diagnostic results, run the above-mentioned command

Parameter

Parameter	Description
Port	Stands for the existent port

Default

None

Usage Guidelines

This command can be executed in EXEC mode to browse the cable diagnostic results of a port

Example

The following example shows the cable diagnostic information of port g0/1.:

When not plugged in, the display is as follows:

Switch_config#show cable interface g0/1

g0/1 cable info:

Cable Open pair (4 pairs)

Pair A Open pair , length 2 metres

Pair B Open pair , length 3 metres

Pair C Open pair , length 2 metres

Pair D Open pair , length 2 metres

The display after plugging in the cable is as follows:

Switch_config#show cable interface g0/8

g0/8 cable info:

Cable OK (4 pairs)

Pair A OK , length 1 metres

Pair B OK , length 1 metres

Pair C OK , length 1 metres

Pair D OK , length 1 metres

If there is a problem with the cable, errors such as short and crosstalk will be displayed

18.9 Configuration Example

The following example shows how to create a VLAN port, set its description information and IP address and browse the status and settings of this port

Switch_config#

Switch_config# interface vlan1

Switch_config_v1# description uplink

Switch_config_v1#

Switch_config_v1# ip address 192.168.1.1 255.255.255.0

Switch_config_v1# exit

Switch_config#

Switch_config# show running-config interface vlan1

Building configuration...

Current configuration:

```
!
interface VLAN1
  description uplink
  ip address 192.168.1.1 255.255.255.0
Switch_config# show interface vlan1
VLAN1 is up, line protocol is down
    Description uplink
    Hardware is EtherSVI, Address is 00e0.0fe4.d06a(00e0.0fe4.d06a)
    Interface address is 192.168.1.1/24
    MTU 1500 bytes, BW 1000000 kbit, DLY 2000 usec
    Encapsulation ARPA
    ARP type: ARPA, ARP timeout 04:00:00
    Peak input rate 0 pps, output 0 pps
        0 packets input, 0 bytes
        Received 0 broadcasts, 0 multicasts
        0 mpls unicasts, 0 mpls multicasts, 0 mpls input discards
        0 input errors, 0 input discards
        0 packets output, 0 bytes
        Transmited 0 broadcasts, 0 multicasts
        0 mpls unicasts, 0 mpls multicasts, 0 mpls output discards
        0 output errors, 0 discards
Switch_config#
```

Chapter 19 Interface Physical Characteristic Configuration Commands

19.1 speed

Syntax

speed {*10* | *100* | *auto*} (RJ45port)

speed {*100* | *1000* | *auto*} (SFP port)

no speed

To configure the speed for the interface, use the **speed** command

Parameter

Parameter	Description
10, 100,1000	Configures the interface speed as 10M, 100M, 1000M
auto	Enable the auto-negotiation capability of the interface

Default

TX interface is auto-negotiation operation, 100M optical interface speed is 100M, gigabit optical interface speed is 1000M

Usage Guidelines

Use this command in the layer 2 interface configuration mode

Note:

The speed of the optical interface is fixed. By default, the auto-negotiation function on the Gigabit optical interface is enabled. The combo port does not support forced gigabit and full duplex simultaneously. Ordinary TX interface does not support speed 1000

Example

The following example sets the interface g0/1 speed to 100M:

Switch_config# interface g0/1

Switch_config_g0/1# speed 100

19.2 duplex

Syntax

duplex {*auto* | *full* | *half*}

no duplex

To configure the duplex operation on an interface, use the duplex command

Parameter

Parameter	Description
auto	Specifies the auto-negotiation operation
full	Specifies the full-duplex operation
half	Specifies the half-duplex operation

Default

TX interface is auto-negotiation operation, optical interface is full-duplex operation

Usage Guidelines

Use this command in the layer 2 configuration mode

Note:

THE DUPLEX OPERATION OF THE OPTICAL INTERFACE IS FIXED, THAT IS FULL-DUPLEX OPERATION. THE COMBO PORT DOESN'T SUPPORT BOTH GIGABIT AND FULL-DUPLEX OPERATION. IN HALF-DUPLEX MODE, BACK PRESSURE OCCURS

Example

The following example configures interface g0/1 to full-duplex operation:

Switch_config# interface g0/1

Switch_config_g0/1# duplex full

19.3 flow-control

Syntax

flow-control { **on | off | auto**}

To configure flow control on an interface, use the flow control command

Parameter

Parameter	Description
on	Enables flow control
off	Disables flow control

auto	Auto-negotiation mode

Default

Disabled

Usage Guidelines

Use this command in the layer 2 configuration mode

Note:

Both “flow-control auto” and “flow-control on” are forced to receive flow-control frame. But in “auto” mode, the flow-control frame is sent only after successful negotiation with the opposite end

Example

The following example enables the flow-control on the g0/1 interface:

Switch_config#int g0/1

Switch_config_g0/1#flow-control on

Chapter 20 Interface Range Command

20.1 Interface Range

Syntax

interface range *type slot*/<*port1-port2* | *port3*>[, <*port1-port2*|*port3*>]

Parameter

Name	Description	Range
type	Port type	All legal port types, except management ports on the main board of the rackmount switch
slot	Slot number	All legal slot number
port1	Beginning value of the port number	All legal port numbers on the slot
port2	Ending value of the port number	All legal port numbers on the slot except for port 1
port3	A single port.	All legal port numbers on the slot

Default

None

Usage Guidelines

Use this command to enter the interface range mode

Example

Use the following command to enter the enterface configuration mode, including the Ethernet ports 1, 2, 3 and 4:

switch_config# interface range gigaEthernet 0/1-4

switch_config_if_range#

Note:

THERE ARE NO SPACE ON EITHER SIDE OF "-" AND ","

Chapter 21 Configuring Physical Interface IP Access List Command

21.1 ip access-group

Syntax

To apply an access control list to control packet access, use the ip access-group command in the appropriate configuration mode. To remove the specified access group, use the no form of this command

In interface configuration mode:

[**no**] **ip access-group** *name*

In global configuration mode:

[**no**] **ip access-group** *name* [**vlan** {*word* | **add** *word* | **remove** *word*}]

Enable the IP access list that created on the port or global, or remove the IP access list that applied on the port or global

Parameter

Parameter	Description
name	Name of an IP access list
Vlan	Apply the access list on inbound of VLAN
Word	VLAN range table
add	Add VLAN range table
remove	Remove VLAN range table

Command Mode

Global configuration mode or interface configuration mode

Usage Guidelines

Most of the commands in the access list are configured by hardware. The commands that are not supported by hardware do not prompt errors, but have no actual effect. A small amount commands such as time-range is configured by software

Note:

Ipv4 standard access list support:

Any: any source ip address

source-addr source-mask : source address matching

reverse-mask source-addr source-mask: reverse mask source address matching

ipv4 extended access list support:

any: any ip address

Ip-protocol: IP protocol number

ip -IP protocol

reverse-mask -protocols for the reverse mask configuration

eq/gt/lt/src-portrange/ dst-portrange: tcp/udp port number matching

gre: GRE protocol number matching

icmp: ICMP protocol number matching

igmp: IGMP protocol number matching

ospf: OSPF touting protocol number matching

tcp/udp port number matching can configure source port number matching and destination port number matching at the same time, but only the destination port number matching takes effect. However, if one of the matching methods is eq, the source port number matching and destination port number matching can take effect at the same time

Example

The following example applies access list filter on packets inbound from Ethernet interface g0/1:

Switch_config#inter g0/1

Switch_config_g0/1# ip access-group filter

21.2 ipv6 access-group

Syntax

To apply an access control list to control packet access, use the ipv6 access-group command in the port configuration mode. To remove the specified access group, use the no form of this command

In interface configuration mode:

[**no**] **ip access-group** *name*

In global configuration mode:

[**no**] **ipv6 access-group** *name* **[vlan {***word* **| add** *word* **| remove** *word***}]**

Enable the IP6 access list that created on the port or global, or remove the IP6 access list that applied on the port or global

Parameter

Parameter	Description
name	Name of an IP access list

Vlan	Apply the access list on inbound of VLAN
Word	VLAN range table
add	Add VLAN range table
remove	Remove VLAN range table

Command mode

Global configuration mode or interface configuration mode

Usage Guidelines

Most of the commands in the access list are configured by hardware. The commands that are not supported by hardware do not prompt errors, but have no actual effect. A small amount commands such as time-range is configured by software

Note:

Ipv6 access list support:

Any: any ipv6 address

Ipv6-addr/ host *Ipv6-addr:* ipv6 address matching

Ipv6-protocol: ipv6 protocol number

eq/gt/lt/src-port-range/ dst-port-range: tcp/udp port number matching

dscp/flow-label: packets flied matching

tcp/udp port number matching can configure source port number matching and destination port number matching at the same time, but only the destination port number matching takes effect. However, if one of the matching methods is eq, the source port number matching and destination port number matching can take effect at the same time

Example

The following example applies access list filter on packets inbound from Ethernet interface g0/1:

Switch_config#inter g0/1

Switch_config_g0/1# ipv6 access-group filter

Chapter 22 IP Hardware Subnet Routing Configuration Commands

22.1 ip exf

Syntax

[no] ip exf

Parameter

N/A

Default value

Enable

Command mode

Global configuration mode

Usage guidelines

The IP hardware subnet routing function can be enabled through this command. If this function is not enabled, the hardware forwarding items can still be configured but they invalidates

Example

The following example shows how to enable the IP hardware subnet route

Switch_config#ip exf

22.2 ip exf down-up-threshold

Syntax

ip exf down-up-threshold *rate*

no ip exf down-up-threshold

Parameter

Name	Usage guidelines
down-up-threshold *rate*	Stands for the trigger value (percent) of hardware subnet routing switch

Default value

90

Command mode

Global configuration mode

Usage guidelines

When the number of software routes exceeds the trigger value of hardware subnet routing, the hardware subnet routing will be shut down; when the number of software routes lowers to be less than the trigger value, the hardware subnet routing will be opened again

Example

The following example shows how to enable the hardware subnet routing on a L3 switch and set the trigger value to 80%

ip exf down-up-threshold 80

22.3 debug ip exf

Syntax

[no] debug ip exf

Parameter

N/A

Default value

N/A

Command mode

EXEC

Usage guidelines

It is used to enable or disable the debugging switch of IP EXF

Example

The following are examples of common debugging information output

2004-7-30 15:50:40 [EXF]: EXF entry(destination 2.10.0.0/16) delete from hardware table, EXF disabled

It means that user enters the no ip exf command and all exf items invalidate

2004-7-30 15:50:44 [EXF]: EXF entry(destination 2.10.0.0/16) add to hardware, NAT enabled, nexthop CPU

It means that the NAT function is enabled at the port where the next hop of the configured exf item belongs. In this case, the packet of the exf item is transmitted to CPU for processing

2004-7-30 15:52:03 [EXF]: EXF entry(destination 2.9.0.0/16) add to hardware, no ARP, nexthop CPU

It means that the ARP of the IP address of the next hop of the configured exf item is not learned. In this case, the packet of the exf item is transmitted to CPU for processing

2004-7-30 15:50:44 [EXF]: EXF entry(destination 2.3.0.0/16) add to hardware sucessfully

It means that the EXF entry is configured successfully

2004-7-30 15:56:00 [EXF]: EXF entry(destination 2.2.0.0/16) delete from hardware table by command

It means that the EXF entry is deleted through the corresponding command

2004-7-30 15:56:59 [EXF]: EXF entry(destination 2.3.0.0/16) delete from hardware table, delete by interface

It means that the interface for the next hop of the configured EXF entry is down or the EXF entry becomes invalid because of NAT settings

Chapter 23 IP-Attack Prevention Configuration Commands

23.1 IP-Attack Prevention Configuration Commands

23.1.1 ip verify icmp ping-flood

Syntax

TO RESTRICT PING PACKET RECEPTION, USE THE ABOVE COMMAND.

Parameter

Parameter	Description
<1 - 50000>	The number of packets with the same source address allowed to be received per second, exceeding this threshold is considered as an attack

Default

Default is 300 ping packets per second per source address

Command mode

Global configuration mode

Example

switch_config#ip verify icmp ping-flood 500

switch_config#ip verify icmp ping-flood

Related command

ip verify icmp ping-sweep

23.1.2 ip verify icmp ping-sweep

Syntax

TO RESTRICT PING SCANNING, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 60>	Anti-attack detection cycle. During this period, the destination address of the ping packet that is more than one scan unit is considered an attack

Note:

One scan unit means that the hash value of the number of changes in address or port exceeds an internal rating

Default

The default detection period is 3 seconds

Command mode

Global configuration mode

Example

switch_config#ip verify icmp ping-sweep 2

switch_config#ip verify icmp ping-sweep

Related command

ip verify icmp ping-flood

23.1.3 ip verify tcp syn-flood

Syntax

TO RESTRICT TCP SYN PACKET RECEPTION, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 50000>	The number of packets with the same source address allowed to be received per second, exceeding this threshold is considered as an attack

Default

Default is 300 tcp syn packets per second per source address

Command mode

Global configuration mode

Example

switch_config#ip verify tcp syn-flood 100

switch_config#ip verify tcp syn-flood

Related command

ip verify tcp syn-sweep

ip verify tcp fin-scan

ip verify tcp rst-flood

23.1.4 ip verify tcp syn-sweep

Syntax

TO RESTRICT TCP SYN PORT SCANNING, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 60>	Anti-attack detection cycle. During this period, the destination port of the tcp syn packet that is more than one scan unit is considered an attack

Default

The default detection period is 3 seconds

Command mode

Global configuration mode

Example

switch_config#ip verify tcp syn-sweep 10

switch_config#ip verify tcp syn-sweep

Related command

ip verify tcp syn-flood

ip verify tcp fin-scan

ip verify tcp rst-flood

23.1.5 ip verify tcp fin-scan

Syntax

TO RESTRICT TCP STEALTH FIN SCANNING, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 60>	Anti-attack detection cycle. During this period, the destination port of the tcp fin packet that is more than one scan unit is considered an attack

Default

The default detection period is 3 seconds

Command mode

Global configuration mode

Example

switch_config#ip verify tcp fin-scan 10

switch_config#ip verify tcp fin-scan

Related command

ip verify tcp syn-flood

ip verify tcp syn-sweep

ip verify tcp rst-flood

23.1.6 ip verify tcp rst-flood

Syntax

TO RESTRICT TCP RST PACKET RECEPTION, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 50000>	The number of packets with the same source address allowed to be received per second, exceeding this threshold is considered as an attack

Default

Default is 300 tcp rst packets per second per source address

Command mode

Global configuration mode

Example

switch_config#ip verify tcp rst-flood 200

switch_config#ip verify tcp rst-flood

Related command

ip verify tcp syn-flood

ip verify tcp syn-sweep

ip verify tcp fin-scan

23.1.7 ip verify udp udp-flood

Syntax

TO RESTRICT UDP PACKET RECEPTION, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 50000>	The number of packets with the same source address allowed to be received per second, exceeding this threshold is considered as an attack

Default

Default is 300 udp packets per second per source address

Command mode

Global configuration mode

Example

switch_config#ip verify udp udp-flood 200

switch_config#ip verify udp udp-flood

Related command

ip verify udp udp-sweep

23.1.8 ip verify udp udp-sweep

Syntax

TO RESTRICT UDP SCANNING, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 60>	Anti-attack detection cycle. During this period, the destination port of the tcp fin packet that is more than one scan unit is considered as an attack

Default

The default detection period is 3 seconds

Command mode

Global configuration mode

Example

switch_config#ip verify udp udp-sweep 10

switch_config#ip verify udp udp-sweep

Related command

ip verify udp udp-flood

23.1.9 ip verify attack Xmas-Tree

Syntax

TO FILTER XMAS-TREE SCAN ATTACKS, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 60>	Anti-attack detection cycle. During this period, tcp fin packets are found with **urg** and **push** flags, and the destination port is more than one scan unit is considered as an attack

Default

The default detection period is 3 seconds

Command mode

Global configuration mode

Example

switch_config#ip verify attack Xmas-Tree 10

switch_config#ip verify attack Xmas-Tree

Related command

ip verify attack Null-scan

ip verify attack Land

ip verify attack Smurf

ip verify attack WinNuke

ip verify attack Ping-of-Death

ip verify attack TearDrop

ip verify attack Fraggle

23.1.10 ip verify attack Null-scan

Syntax

TO FILTER NULL SCAN ATTACK, USE THE ABOVE COMMAND

Parameter

Parameter	Description
<1 - 60>	Anti-attack detection cycle. During this period, tcp packets carry an empty flag, and the destination port is more than one scan unit is considered as an attack

Default

The default detection period is 3 seconds

Command mode

Global configuration mode

Example

switch_config#ip verify attack Null-scan 10

switch_config#ip verify attack Null-scan

Related command

ip verify attack Xmas-Tree

ip verify attack Land

ip verify attack Smurf

ip verify attack WinNuke

ip verify attack Ping-of-Death

ip verify attack TearDrop

ip verify attack Fraggle

23.1.11 ip verify attack Land

Syntax

TO FILTER LAND ATTACKS, USE THE ABOVE COMMAND

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify attack Land

Related command

ip verify attack Xmas-Tree

ip verify attack Null-scan

ip verify attack Smurf

ip verify attack WinNuke

ip verify attack Ping-of-Death

ip verify attack TearDrop

ip verify attack Fraggle

23.1.12 ip verify attack Smurf

Syntax

TO FILTER SMURF ATTACKS, USE THE ABOVE COMMAND

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify attack Smurf

Related command

ip verify attack Xmas-Tree

ip verify attack Null-scan

ip verify attack Land

ip verify attack WinNuke

ip verify attack Ping-of-Death

ip verify attack TearDrop

ip verify attack Fraggle

23.1.13 ip verify attack WinNuke

Syntax

TO FILTER WINNUKE ATTACKS, USE THE ABOVE COMMAND

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify attack WinNuke

Related command

ip verify attack Xmas-Tree

ip verify attack Null-scan

ip verify attack Land

ip verify attack Smurf

ip verify attack Ping-of-Death

ip verify attack TearDrop

ip verify attack Fraggle

23.1.14 ip verify attack TearDrop

Syntax

TO FILTER TEARDROP ATTACKS, USE THE ABOVE COMMAND.

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify attack TearDrop

Related command

ip verify attack Xmas-Tree

ip verify attack Null-scan

ip verify attack Land

ip verify attack Smurf

ip verify attack WinNuke

ip verify attack Ping-of-Death

ip verify attack Fraggle

23.1.15 ip verify attack Fraggle

Syntax

TO FILTER FRAGGLE ATTACKS, USE THE ABOVE COMMAND

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify attack Fraggle

Related command

ip verify attack Xmas-Tree

ip verify attack Null-scan

ip verify attack Land

ip verify attack Smurf

ip verify attack WinNuke

ip verify attack Ping-of-Death

ip verify attack TearDrop

23.1.16 ip verify all

Syntax

TO FILTER ALL ATTACKS, USE THE ABOVE COMMAND

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify all

switch_config#no ip verify all

Related command

ip verify icmp ping-flood

ip verify icmp ping-sweep

ip verify tcp syn-flood

ip verify tcp syn-sweep

ip verify tcp fin-scan

ip verify tcp rst-flood

ip verify udp udp-flood

ip verify udp udp-sweep

ip verify attack Xmas-Tree

ip verify attack Null-scan

ip verify attack Land

ip verify attack Smurf

ip verify attack WinNuke

ip verify attack TearDrop

ip verify attack Fraggle

23.1.17 ip verify filter

Syntax

TO FILTER PACKETS, USE THE ABOVE COMMAND. AFTER AN ATTACK HAS OCCURRED, DISCARD THE PACKET THAT CAUSED THE ATTACK FOR A DURATION OF 3 MINUTES

Parameter

Parameter	Description
<30 - 43200>	Stands for the time (in seconds) to block the attack source after detecting an attack. Up to 12 hours

Default

Default blocking time is 180 seconds

Command mode

Global configuration mode

Example

switch_config#ip verify filter 600

switch_config#no ip verify filter

Related command

None

23.1.18 ip verify enable

Syntax

TO ENABLE/DISABLE ATTACK PROTECTION, USE THE ABOVE COMMAND.

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify enable

switch_config#no ip verify enable

Related command

None

23.1.19 ip verify log-enable

Syntax

TO ENABLE THE ATTACK PROTECTION LOG, USE THE ABOVE COMMAND. AFTER AN ATTACK HAS OCCURRED, THE RELEVANT SYSTEM LOG IS OUTPUT.

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify log-enable

switch_config#no ip verify log-enable

Related command

ip verify enable

23.1.20 show ip table

Syntax

TO DISPLAY CURRENT IP DATA FLOW TABLE, USE THE ABOVE COMMAND.

Parameter

None

Command mode

Non-user mode

Example

#show ip table

No.	Src-address	Dst-address	Timer
0	90.0.0.3	90.0.0.33	80
1	90.0.0.33	224.0.0.1	71
2	90.0.0.33	224.0.0.13	57

23.1.21 show ip table src

Syntax

TO DISPLAY THE CURRENT IP SOURCE ADDRESS INDEX TABLE, USE THE ABOVE COMMAND

Parameter

None

Command mode

Non-user mode

Example

#show ip table src

No.	Src-address	Flows	Flags
0	90.0.0.3	1	0x200
1	90.0.0.33	2	0

Flows: indicates the index of the data flow to which the IP source address belongs.

Flags: records the attack type of the IP source address

Chapter 24 IP Direct Network Segment Scanning Attack Protection Configuration Commands

24.1 IP Direct Network Segment Scanning Attack Protection Configuration Commands

24.1.1 ip verify ip-sweep detect unknown-host

Syntax

Enable/disable the anti-attack function for IP scanning of unidentified hosts on the directly connected network. When a certain number of incomplete arps are hit under a certain vlan, it is considered to have received an IP directly connected network segment scanning attack. The measures of **rate-limit** and **rate-limit-attacker** cannot be enabled at the same time

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config#ip verify ip-sweep detect unknown-host

Related command

ip verify ip-sweep action

24.1.2 ip verify ip-sweep action rate-limit

Syntax

TO LIMIT THE SPEED OF ALL IP PACKETS, USE THE ABOVE COMMAND. OPTIONAL PARAMETER INCLUDES LIMIT OF THE WINDOW TIME AND THE NUMBER OF PACKETS.

Parameter

Parameter	Description
<1 - 5>	Limit the time window size of IP packets (seconds)
<1 - 5000>	Number of IP packets allowed to be received in the time window

Precautions

1. When the window time is reached, the number of passing IP packets will be specified again. The current limit is only limited to the packets sent to the CPU, and the IP packets that the hardware has learned to cache cannot be restricted

2. **ip verify ip-sweep action rate-limit** cannot be configured when **ip verify action rate-limit-attacker** is configured

Default

Disabled by default

When configuring this function without the optional parameter, the default window time is 1 second, and the default received IP packets are 200

Command mode

Global configuration mode

Example

switch_config# ip verify ip-sweep action rate-limit 2 500

Related command

ip verify ip-sweep action rate-limit-attacker

24.1.3 ip verify ip-sweep action rate-limit-attacker

Syntax

TO ENABLE RATE LIMIT OF ALL IP PACKETS THAT ARE DETECTED AS ATTACKERS, USE THE ABOVE COMMAND. OPTIONAL PARAMETER INCLUDES LIMIT OF THE WINDOW TIME AND THE NUMBER OF PACKETS

THIS COMMAND WILL OVERRIDE THE EFFECT OF THE IP VERIFY IP-SWEEP ACTION RATE-LIMIT **COMMAND**

Parameter

Parameter	Description
<1 - 5>	Limit the time window size of IP packets (seconds)
<1 - 5000>	Number of IP packets allowed to be received in the time window

Default

Disabled by default

When configuring the command without the optional Parameter, if the time window and number of packets are configured with the **ip verify action rate-limit** command, the default window time and the number of

packets will inherit this value. If not configured, the default window time is 1 second, and the default received IP packets are 200

Command mode

Global configuration mode

Example

switch_config# ip verify ip-sweep action rate-limit-attacker 2 1000

Related command

ip verify ip-sweep action rate-limit

24.1.4 ip verify ip-sweep action no-cache

Syntax

TO PROHIBIT THE CREATION OF CACHES FOR UNIDENTIFIED HOSTS ON DIRECTLY CONNECTED NETWORKS, AND DELETE THE SOFTWARE CACHE THAT CONTINUOUSLY FLOWS TO UNIDENTIFIED HOSTS, USE THE ABOVE COMMAND

Parameter

None

Default

Disabled

Command mode

Global configuration mode

Example

switch_config# ip verify ip-sweep action no-cache

Note

Currently only prohibited:

1. The destination outlet is an incomplete arp stream

2. When the number of incomplete arps reaches the upper limit, it is forbidden to create a cache for a stream without corresponding arp

When the number of incomplete arps is not yet full and there is no corresponding stream generated by arp, you are allowed to create a cache

24.1.5 show ip verify config

Syntax

To display the current configuration of IP directly connected network segment scanning anti-attack detection, use the above command

Parameter

None

Command mode

Non-user mode

Example

```
switch_config# show ip verify config
IP-sweep unknown-host                    : Enabled
IP-sweep action logging                  : Enabled
IP-sweep action no-cache                 : Disabled
IP-sweep action rate-limit               : Enabled
IP-sweep action rate-limit-attacker: Disabled
Rate-limit time-window in unit of second    : 1
Number of packets allowed every time-window: 200
IP-sweep filter time                        : 180
```

Note: The switch interface is aligned, the word display is not neat

24.1.6 show ip verify status

Syntax

To shows whether the IP-direct network segment scanning anti-attack detection is enabled, whether it has received an attack, and details of the attacker, use the above command

Parameter

None

Command mode

Non-user mode

Example

```
switch_config# show ip verify status
Detection for Unknown-host(connected network sweep) attack configured
Unknown-host(connected network sweep) attack detected
Number of Unknown-host(connected network sweep) attackers: 1
  Attacker 100.1.1.10, count 32, VLAN 100, port g2/1
```

Chapter 25 IP-PBR Configuration Commands

25.1 ip pbr

Description

ip pbr

no ip pbr

Parameter

None

Default value

The IP-PBR function is disabled by default

Description

It is used to enable or disable the IP-PBR function. The no ip pbr command is used to resume the default value

Example

switch_config# ip pbr

switch_config#

25.2 show ip pbr

Description

show ip pbr

Parameter

None

Default value

None

Description

It is used to display the information about RIP configuration

Example

The following example shows how to display the information about IP-PBR running

switch_config# show ip pbr

IP policy based route state: enabled

No equiv exf apply item

VLAN3 use route-map ddd, and has 1 entry active

Entry sequence 10, permit

Match ip access-list:

ac1

Set Outgoing nexthop

90.0.0.3

switch_config#

25.3 show ip pbr policy

Description

show ip pbr policy

Parameter

None

Default value

None

Description

It is used to display the information about RIP configuration

Example

The following example shows how to display the information about IP-PBR policy routing configuration

IP policy based route state: enabled

VLAN3 use route-map ddd, and has 1 entry active

Entry sequence 10, permit

Match ip access-list:

ac1

Set Outgoing nexthop

90.0.0.3

switch_config#

25.4 show ip pbr exf

Description

show ip pbr exf

Parameter

None

Default value

None

Description

It is used to display the information about IP-PBR equivalent routing

Example

The following example shows how to display the information about IP-PBR equivalent routing

switch_config# show ip pbr exf

IP policy based route state: enabled

Equiv EXF has 1 entry active

Entry sequence 1, handle c1f95b0

Dest ip: 1.1.0.0/16

90.0.0.3

192.168.213.161

switch_config#

25.5 debug ip pbr

Description

debug ip pbr

no debug ip pbr

Parameter

None

Default value

None

Description

It is used to enable or disable the debugging switch of IP-PBR

Example

The following example shows how to enable the debugging switch of IP-PBR

switch # debug ip pbr

Chapter 26 IPv6 ACL Configuration Commands

This chapter describes the commands and methods used to configure IPv6 ACL, which are used to control user access to the network. The command mainly includes three parts: Deny, Permit and Sequence.

IPv6 ACL Configuration Commands include:

Command	Description
ipv6 access-list	Establish standard and extended IPv6 access lists
ipv6 access-group	Apply access list to port
deny/permit	Filter packets.
sequnence	Configure access list sequence number
show ipv6 access-list	Show the configured access list

26.1 IPv6 ACL Configuration Commands

26.1.1 ipv6 access-list

Syntax

To configure the name of access list and enter IPv6 ACL configuration mode, run the following command. To return to the default setting, use the no form of this command after exiting the access list configuration mode with the **exit** command

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Parameter

Parameter	Description
access-list-name	access list name

Default value

There is no default access list. There must be configured with access list name

Command mode

Global configuration mode. The command is used to enter IPv6 access control list configuration mode.

Usage guidelines

1. IPv6 will not use number access list and the number will also be handled as name access list. The access list of IPv4 and IPv6 cannot use the same name, or the port cannot be identified
2. The default configuration of IPv6 ACL is to enable ND packets of ICMPv6 (equivalent to ARP of IPv4). That's, when using deny configuration rule, add permit any any to the last command. The rules as follows:

permit icmpv6 any any nd-na

permit icmpv6 any any nd-ns

deny ipv6 any any

Example

The following example shows how to create an IPv6 access control list. Use deny to deny packets whose source address prefix is FEC0:0:0:2::/64 and whose destination address is any. Meanwhile, other packets are permitted and apply the command to gigabit Ethernet interface G1/1

ipv6 access-list list2

deny FEC0:0:0:2::/64 any

permit ipv6 any any

interface G1/1

ipv6 access-group list2 egress

Related command

deny (IPv6)

permit (IPv6)

ipv6 access-group

show ipv6 access-list

26.1.2 ipv6 access-group

Syntax

To designate an access group to a specific vlan port, run the ipv6 access-group. To cancel the designated access group, run no ipv6 access-group

ipv6 access-group *access-list-name* {**in | out**}

no ipv6 access-group *access-list-name*

Parameters

Parameters	Description
access-list-name	Name of the IP access control list
in	Filter incoming packets
out	Filter leaving packets

Default value

There is no default access list, you must configure a specific access list name to the specified port to be effective

Command Mode

Vlan port configuration mode

Usage Guidelines

The command **ipv6 access-group** filters the packets forwarded by the switch, not the packets generated by the switch itself

Example

The following example applies the access list rule "example" to the leaving packet under the vlan port

Switch_config#interface vlan 4

Switch_config_v4#ipv6 access-group example out

Related command

ipv6 access-list

show ipv6 access-list

26.1.3 deny/permit

Syntax

To deny certain packets, run the following command. To return to the default setting, use the no form of this command

deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

no deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

deny icmpv6 {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]]

{*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]

deny tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**routing**] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

deny udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [**sequence** *value*] [**time-range** *name*]

Green color: deny fields which protocol, deny icmp, deny tcp and deny udp have

Red color: deny fields which deny protocol has but deny icmp, deny tcp or deny udp hasn't; neither permit

Blue: deny fields which deny protocol hasn't but deny icmp, deny tcp or deny udp has

For enabled packets, use command permit and other related setting rule of permit. Use the no form of this command to return to the default setting

permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

no permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

permit icmpv6 {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*icmpv6-type* [*icmpv6-code*] | *icmpv6-message*] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]

permit tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**routing**] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

permit udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [**sequence** *value*] [**time-range** *name*]

Parameter

Parameter	Description
protocol	Network protocol name or protocol number. The current supported protocol name are ahp(51), esp(50), icmpv6(58), ipv6(41), pcp(108), sctp(132), tcp(6), udp(17)
source-ipv6-prefix/prefixlength	Source IPv6 prefix/prefix length
any	Abbreviation of IPv6 prefix ::/0

host *source-ipv6-address*	Source IPv6 host address
operator [*port-number*]	(optional) operational character and port number are only effective for tcp and udp protocol. Operator has **lt** (less than), **gt** (greater than), **eq** (equal), **neq**(not equal) and **range**(inclusive range). The operator **range** has two port numbers and other operators only have one port number. The value range of *port-number* is 0 to 65535
destination-ipv6-prefix/*prefix-length*	Destination IPv6 prefix/prefix length
host *destination-ipv6-address*	Destination IPv6 host address
dscp *value*	(optional) differentiated services code point (dscp, differentiated services code point). It is used for matching IPv6 packet header Traffic Class domain, 0-63. The existed definitions are af11(001010), af12(001100), af13(001110), af21(010010), af22(010100), af23(010110), af31(011010), af32(011100), af33(011110), af41(100010), af42(100100), af43(100110), cs1(001000), cs2(010000), cs3(011000), cs4(100000), cs5(101000), cs6(110000), cs7(111000), ef(101110), default(000000)
flow-label *value*	(optional) Flow label of IPv6 packet header, 1-1048575(1024*1024-1)
fragments	If the fragment header has non-0 offset, it will match the non-initiated fragment header group. Only ***operator*** **[*port-number*]** does not be claimed, **fragments** are optional
log	(optional) When grouping match, send log information to the console port. The log information includes access list name, serial number, grouping deny/permit, protocol/protocol number (TCP, UDP, ICMPv6, etc.), source address/destination address, source port number/destination port number
log-input	(optional) It has the same function with log. It also includes packet ingress
routing	(optional) Matching the route extended header of IPv6 grouping
sequence *value*	(optional) It is used to designate the serial number of the access list, which is easy for the client to add 1-4294967295 (65536*65536-1). IPv4 access list can only add the rule to the last, while IPv6 can add the rule to any position by make use of sequence. If there is rule on the position of new added sequence number, the rule will be overlapped
time-range *name*	(optional) Set the time range of the access list. In command **time-range**, apply time rule name to the access list with the key words **absolute/periodic**
undetermined-transport	(optional) Match grouping which layer-4 protocol cannot distinguish. Only protocol is not claimed, can **undetermined-transport** is optional. If protocol is ipv6, it means that layer-4 protocol of IPv6 is not claimed
icmpv6-type	(optional) Packet type of ICMPv6, 0-255
icmpv6-code	(optional) ICMPv6 packet code, 0-255
icmpv6-message	(optional) pass ICMPv6 packet name (RFC specified packet name and ICMP packet type constituted by the packet code, such as destination unreachable), 0 to 255
ack	(optional) Used only for TCP packets, acknowledgment (ACK) setting

fin	(optional) Used only for TCP packets, finish (FIN) matching
psh	(optional) Used only for TCP packets, push (PSH) set
rst	(optional) Used only for TCP packets, reset (RST) set
syn	(optional) Used only for TCP packets, synchronize (SYN) matching set
urg	Used only for TCP packets, urgent (URG) matching set
established	(optional) Used only for TCP packets. When ACK or RST of TCP packets are set, it means the match is established. When the rule is used as deny, it is used to deny the connection from external network to inner network, but enables connection from inner network to the external network
eq{*port* | *protocol*}	(optional) Used only for grouping of designated port number. Protocol is the designated protocol name
gt{*port* | *protocol*}	(optional) Used only for grouping greater than the designated port number. Protocol is the designated protocol name
lt {*port* | *protocol*}	(optional) Used only for grouping smaller than the designated port number. Protocol is the designated protocol name.
neq {*port* | *protocol*}	(optional) Only matching with grouping not in the designated port number. Protocol is the designated protocol name
range {*port* | *protocol*}	(optional) Only matching with grouping in the designated port number. Protocol is the designated protocol name

Default value

1. Serial number:

Different with ACL of IPv4, ACL of IPv6 can add in any position of the existed access list with **permit, deny and sequence**, not only limited to the end of ACL. Therefore, the access list needs to be numbered. If the user does not configure the sequence number of the access list manually, the first default ACL serial No. is 10, add 10 successively; if the user designated sequence number, it will be inserted accordingly; if the user designated sequence number is the same with that of existed ACL, the existed ACL will be overlapped. If the last sequence number designated by the user is not an integral multiple of 10, when ACL rule is added without designating the sequence number, the sequence number will be the sequence number of the last rule plus 10

2. Default rule

Similar to IPv4 ACL, if configured ACL name, but without configuring the rule, the access list will not disable any rule.

permit icmpv6 any any nd-na

permit icmpv6 any any nd-ns

permit ipv6 any any

It should be noted that as ICMP of IPv6 is equivalent to ARP of IPv4, the neighbor inform and neighbor request of the neighbor discovery can pass by default. If one rule is configured in IPv6 ACL rule, the implied condition of disqualifying the rule is to enable ICMPv6 packets, but disable all IPv6 packets

permit icmp any any nd-na

permit icmp any any nd-ns

deny ipv6 any any

Therefore, if enable packets disqualifying the rule is disabled, add to IPv6 ACL one command: **permit ipv6 any any**

Command mode

IPv6 access list configuration mode

Usage guidelines

1. Packet name of ICMPv6 as follows:

• beyond-scope

• destination-unreachable

• echo-reply

• echo-request

• header

• hop-limit

• mld-query

• mld-reduction

• mld-report

• nd-na

• nd-ns

• next-header

• no-admin

• no-route

• packet-too-big

• parameter-option

• parameter-problem

• port-unreachable

• reassembly-timeout

• renum-command

• renum-result

• renum-seq-number

• router-advertisement

• router-renumbering

• router-solicitation

• time-exceeded

• unreachable

2. Defined protocols on TCP port number:

• bgp(179)

• chargen(19)

• cmd(514)

• daytime(13)

• discard(9)

• domain(53)

• echo(7)

• exec(512)

• finger(79)

• ftp(21)

• ftp-data (20)

• gopher (70)

• hostname (101)

• ident (113)

• irc (194)

• klogin (543)

• kshell (544)

• login (513)

• lpd (515)

• nntp (119)

• pim-auto-rp (496)

• pop2 (109)

• pop3 (110)

• smtp (25)

• sunrpc (111)

• syslog (514)

• talk (517)

• time (37)

• uucp (540)

• whois (43)

• www (80)

3. Defined protocols on UDP port number:

• biff (512)

• bootpc (68)

• bootps (67)

• discard (9)

• dnsix (195)

• domain(53)

• echo(7)

• isakmp (500)

• netbios-dgm (138)

• netbios-ns (137)

• netbios-ss (139)

• ntp (123)

• pim-auto-rp (496)

• rip (520)

• snmp (512)

• snmptrap (162)

• sunrpc (111)

• syslog (514)

• talk (517)

• tftp (69)

• time (37)

• who (513)

• xdmcp (177)

Example

The following example shows how to create an IPv6 access list named “example” and set four rules for it. Rule 1: Deny all tcp connected packets whose port destination port number is bigger than 5000; Rule 2: Deny all udp packets whose source port number is smaller than 5000. Rule 3: Enable all icmpv6 packets; Rule 4: Enable all packets which are not satisfy the rule. Note: When configuring access list, if packets not satisfy the rule are not denied, please add the rule. Lastly, in the interface configuration mode, apply the rule to the egress of Ethernet port g2/1

ipv6 access-list example

deny tcp any any gt 5000

deny udp ::/0 lt 5000 ::/0 log

permit icmpv6 any any

permit any any

int gigaEthernet 2/1

ipv6 access-group example egress

Related command

ipv6 access-list

ipv6 access-group

show ipv6 access-list

list

26.1.4 Sequence

Syntax

To insert a new access list or overlap the existed access list in any position, run the following command. To return to the default setting, use the no form of this command

sequence *value* {**deny | permit**} *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**]

no sequence *value* {**deny | permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**]

sequence {**deny | permit**} **icmpv6** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*icmpv6-type* [*icmpv6-code*] | *icmpv6-message*] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*]

sequence {**deny | permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**ack**] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**routing**] [**rst**] [**syn**] [**time-range** *name*] [**urg**]

sequence {**deny | permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [**time-range** *name*]

Parameter

Reference to deny/permit in 1.1.3, which only puts the key words of sequence in the front

Default value

The same with deny/permit in 1.1.3

Command mode

IPv6 access list configuration mode

Usage guidelines

ACL can be added in any position with permit, deny, remark, evaluate, but not only limited to the end of ACL. Between two existed ingresses add an appropriate ingress number. The default first ACL ingress number is 10 and the subsequent ACL ingress number is 10 increased successively

Keywords of sequence is used for:

If seq is not designated, the first seq=10, increase successively after that;

If seq is designated, ipv6acl without seq will be added to the end, and add 10 to the last seq;

If seq is designated, ipv6acl with seq will inserted in the middle;

If seq is designated, ipv6acl with seq and seq is the same with the current, renew ipv6acl of the seq;

If directly designate seq XXX, it means seq XXX deny 0 any any;

Guidelines of other commands are the same with deny/permit in 1.1.3

Example

The following example shows how to configure as 1.1.3 but only adds the sequence number in the front

ipv6 access-list example

sequence 30 deny tcp any any gt 5000

sequence 70 deny udp ::/0 lt 5000 ::/0 log

sequence 75 permit icmpv6 any any

sequence 76 permit any any

Add a new rule to the existed rule:

deny ipv6 FE80::/64 any log-input

The rule will be added to the end and automatically number the sequence as 76+10=86. If the user designates the sequence number when add the new rule, run the following command:

sequence 50 deny ahp any any

or deny ahp any any sequence 50

The rule will be inserted into rule sequence No.30 and No.70. If the sequence number designated by the user is the same with that of the existed one, run the following command.

sequence 75 deny esp any any log

or deny esp any any log sequence 75

In the existed access list, the rule numbered 75 will be overlapped. Change of the access list adding 3 rules is shown below:

ipv6 access-list example

sequence 30 deny tcp any any gt 5000

sequence 50 deny ahp any any

sequence 70 deny udp ::/0 lt 5000 ::/0 log

sequence 75 deny esp any any log

sequence 76 permit any any

deny ipv6 FE80::/64 any log-input sequence 86

Related command

deny(IPv6)

permit(IPv6)

ipv6 access-list

ipv6 access-group

show ipv6 access-list

list

26.1.5 show ipv6 access-list

To show IPv6 ACL information, run the following command.

show ipv6 access-list [*access-list-name*]

Parameter

Parameter	Description
access-list-name	access list name

Default value

If there is no access list input, all access lists will be shown

Command mode

Global configuration mode or EXEC

Usage guidelines

The command **show ipv6 access-list** is used to show the format of IPv6 access list, which is different with the command **show running** for showing the format of IPv6 ACL. When using the command **show running**, the rule with designated sequence number will be shown in the beginning, otherwise, it will be shown in the end. Reference to example in 1.1.4. When using command **show ipv6 access-list**, whether designated the sequence number, the rule with sequence number will be shown in the end. Refer to example in this section

Example

The following example shows how to show example 1 and example 2 by entering the command **show ipv6 access-list**

ipv6 access-list example1

permit ipv6 any any sequence 10

deny icmpv6 any any 255 255 routing sequence 20

ipv6 access-list example2

permit icmpv6 12::/0 host 34:: header dscp ef fragments sequence 20

permit icmpv6 any any header flow-label 987 sequence 30

deny ahp any any routing log time-range example_TIMER sequence 50

deny icmpv6 any any 255 255 sequence 8918

permit any any sequence 8928

Enter command **show ipv6 access-list example1** and show example 1.

ipv6 access-list example1

permit ipv6 any any sequence 10

deny icmpv6 any any 255 255 routing sequence 20

Related command

ipv6 access-list

Chapter 27 IPv6 Configuration Commands

27.1 ipv6 address

Syntax

To set an IPv6 address in port configuration mode and meanwhile enable IPv6 on a port, run **ipv6 address** command. To delete the IPv6 address on a port, run **no ipv6 address** command.

ipv6 address { *ipv6-address/prefix-length* | **general-prefix** *prefix-name sub-bits/prefix-length* }

no ipv6 address [*ipv6-address/prefix-length* | **general-prefix** *prefix-name sub-bits/prefix-length*]

Parameter

Parameter	Description
ipv6-address	Means the to-be-added IPv6 address
/prefix-length	Means the IPv6 prefix' length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address
Prefix-name	Means a general prefix, defining the network part of the IPv6 address
Sub-bits	Means the host part of the IPv6 address. It combines with the prefix, which is defined by prefix-name, to form an IPv6 address. This parameter must support the IPv6 address format regulated in RFC2373

Default

No default IPv6 address exists on the VLAN port

Command Mode

VLAN Interface configuration mode

Usage Guidelines

If you run no ipv6 address, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted

Example

The following example shows how to set an IPv6 address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port

Switch_config_v1# ipv6 address 2001:0:0:0:0DB8:800:200C:417A/64

Related Commands

ipv6 address anycast

ipv6 address eui-64

ipv6 address link-local

show ipv6 interface

27.2 ipv6 address anycast

Syntax

To set an anycast address and enable IPv6 on the VLAN port, run the first one of the following two commands:

ipv6 address *ipv6-prefix/prefix-length* **anycast**

no ipv6 address [*ipv6-prefix/prefix-length* **anycast]**

Parameter

Parameter	Description
Ipv6-prefix	Means the network part of the IPv6 address
/prefix-length	Means the IPv6 prefix length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address

Default

It is set as an anycast address on the VLAN port by default

Command Mode

VLAN Interface configuration mode

Usage Guidelines

If you run no ipv6 address, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted

Example

Switch_config_v1# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast

Related Commands

ipv6 address eui-64

ipv6 address link-local

show ipv6 interface

27.3 ipv6 address autoconfig

Syntax

To use the stateless auto-configuration protocol to set an IPv6 address, run **ipv6 address autoconfig** in VLAN port configuration mode.

Ipv6 address autoconfig

no ipv6 address autoconfig

Parameter

None

Default

By default, IPv6 address auto-configuration is not used

Command Mode

VLAN Interface configuration mode

Example

Switch_config_v1# ipv6 address autoconfig

27.4 ipv6 address eui-64

Syntax

To set an IPv6 address in VLAN port configuration mode, run **ipv6 address eui-64**. To remove the setting, use the no form of the command.

ipv6 address ipv6-prefix/prefix-length eui-64

no ipv6 address [ipv6-prefix/prefix-length eui-64]

Parameter

Parameter	Description
Ipv6-prefix	Means the network part of the IPv6 address
/prefix-length	Means the IPv6 prefix length. It is a decimal value behind the symbol "/", meaning the successive bits in the network part in an address

Default

The IPv6 address in the eui-64 form is not configured on the VLAN port

Command Mode

VLAN Interface configuration mode

Usage Guidelines

If you run no ipv6 address, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted

If the prefix-length parameter is bigger than 64 bits, the prefix-length is prior to the length of the VLAN port ID

Example

Switch_config_v1# ipv6 address 2001:0:0:0:0DB8::/64 eui-64

Related Commands

ipv6 address link-local show
ipv6 interface

27.5 ipv6 address link-local

Syntax

To set a link-local address in VLAN port configuration mode and meanwhile enable IPv6 on the VLAN port, run the first one of the following two commands:

ipv6 address *ipv6-address* **link-local**

no ipv6 address [*ipv6-address* **link-local]**

Parameter

Parameter	Description
ipv6-address	Means the to-be-added IPv6 address. The format of this address must abide by the definition in RFC 4291 strictly
link-local	Means a link-local address. The link-local address designated by the **ipv6-address** command will automatically replace the automatically configured link-local address

Default

No default IPv6 link-local address exists on the VLAN port

Command Mode

Interface configuration mode

Usage Guidelines

If you run **no ipv6 address**, which has no parameters, all manually configured IPv6 addresses on the VLAN port will be deleted. If you run **ipv6 enable**, a link-local address will be automatically set. Of course you can set the link-local address manually, the command you will use is **ipv6 address link-local**

Example

The following example shows how to set a link-local address manually on the VLAN port:

Switch_config_v1# ipv6 address FE80::A00:3EFF:FE12:3457 link-local

Related Commands

ipv6 address eui-64 show
ipv6 interface

27.6 ipv6 enable

Syntax

If the IPv6 address is not set on the VLAN port but users want to enable the IPv6 protocol on this port, run **ipv6 enable**

ipv6 enable

no ipv6 enable

Parameter

None

Default

The IPv6 protocol is forbidden on the VLAN port

Command Mode

VLAN Interface configuration mode

Usage Guidelines

After the **ipv6 enable** command is run, the system will add a link-local address on the VLAN port automatically. At the same time, the communication range of the IPv6 protocol on the VLAN port is confined to the links that the VLAN port connects. If the IPv6 address has already configured on the VLAN port explicitly, you cannot forbid IPv6 processing on the VLAN port even though you use the **no ipv6 enable** command

Example

Switch_config# interface vlan 1

Switch_config_v1# ipv6 enable

Related Commands

ipv6 address link-local ipv6 address eui-64 show ipv6 interface

27.7 show ipv6 interface

Syntax

To show the information about the VLAN port on which the IPv6 protocol is enabled, run the following command:

show ipv6 interface [*interface-type interface-number***] | [brief]**

Parameter

Parameter	Description
interface-type	Stands for the type of the VLAN port
interface-number	Stands for the ID of the VLAN port

Default

Those VLAN ports on which the IPv6 protocol is enabled will all be displayed

Command Mode

Global configuration mode

Usage Guidelines

This command can be used to display the state of IPv6 on the VLAN port, the configured IPv6 address and other IPv6 related parameters

Example

The following example shows how to display the IPv6 state on port vlan1:

Switch# show ipv6 interface vlan 1

Vlan1 is up, line protocol is down

IPv6 is enabled, link-local address is FE80::A00:3EFF:FE12:3457 [TENTATIVE]

Global unicast address(es):

5678::111, subnet is 5678::/64 [TENTATIVE]

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF12:3457

FF02::1:FF00:111

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are enabled

Field	Description
Vlan1 is up(down/administratively down)	Indicates whether the physical layer of the VLAN port is accessible or whether it can be shut down manageably
line protocol is up(down)	Indicates whether the line protocol (the software layer) is accessible
IPv6 is enabled	Enables the IPv6 protocol
link-local address	Displays the link-local address of a port
Globalunicast address(es)	Displays the unicast address of a port
Joinedgroup address(es)	Displays the multicast address of a port
MTU	Displays the MTU of a port
ICMP error messages	Displays the transmission frequency of ICMPv6 error packets (the minimum interval)
ICMP redirects	Displays whether the redirection packet will be sent or not
ICMP unreachables	Displays whether the destination unreachable packet will be enabled or shut down

Related Command

None

Chapter 28 IPv6 Configuration Commands

28.1 clear ipv6 traffic

Syntax

To delete the statistics information about the IPv6 flow, run the following command:

clear ipv6 traffic

Parameter

None

Command Mode

EXEC

Usage Guidelines

This command is used to delete all the statistics information about IPv6 flow

Example

The following example shows how to delete the statistics information about IPv6 flow:

```
Switch# clear ipv6 traffic
Switch# show ipv6 traffic
IPv6 statistics:
Rcvd: 0 total, 0 local destination
0 badhdrs, 0 badvers
0 tooshort, 0 toosmall, 0 toomanyhdrs
0 source-routed, 0 badscope
0 badopts, 0 unknowopts, 0 exthdrtoolong
0 fragments, 0 total reassembled
0 reassembly timeouts, 0 reassembly failures
Sent: 0 generated, 0 forwarded, 0 cant forwarded
0 fragmented into 0 fragments, 0 failed
0 no route
Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 0 total, 0 format errors, 0 checksum errors
  0 unreachable, 0 packet too big
  0 time exceeded, 0 parameter problem
  0 echos, 0 echo replies
  0 membership query, 0 membership report, 0 membership reduction
  0 Switch solicitations, 0 Switch advertisements
  0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
  Sent: 0 total, 0 bandwidth limit
  0 unreachable, 0 packet too big
  0 time exceeded, 0 parameter problem
  0 echos, 0 echo replies
  0 membership query, 0 membership report, 0 membership reduction
```

0 Switch solicitations, 0 Switch advertisements
0 neighbor solicitations, 0 neighbor advertisements, 0 redirect

Related Commands

show ipv6 traffic

28.2 debug ipv6 packet

Syntax

To display the debug information about the IPv6 packet, run the first one of the following two commands:

debug ipv6 packet [interface interface-type interface-number | access-list [access-list-name] | detail]

no debug ipv6 packet

Parameter

Parameter	Description
Interface-type	Type of the interface (optional)
Interface-number	ID of an interface (optional)
access-list-namae	Name of ACL (optional)

Default

The debug information is disabled in default settings

Command Mode

EXEC

Example

The following example shows how to export the IPv6 debug information:

Switch# debug ipv6 packet

2002-1-1 05:07:16

IPv6: source FE80::A00:3EFF:FE12:3459, dest FF02::1

plen 32, proto 58, hops 255

sending on Ethernet1/0

Field	Description

source	Source address in the IPv6 packet
dest	Destination address in the IPv6 packet
plen	Load length in the IPv6 packet
proto	Protocol for the next header encapsulation, which is presented by next-header in the IPv6 packet
hops	Value of hop-limit in the IPv6 packet
sending (receiving, forwarding) on Ethernet	Displays packet transmission, reception and forwarding on an interface

28.3 ipv6 mtu

Syntax

To set the MTU of the VLAN port, run the first one of the following two commands. To return to the default setting, use the no form of this command

ipv6 mtu *bytes*

no ipv6 mtu

Parameter

Parameter	Description
bytes	MTU(unit : byte)

Default

The default value depends on the port type, but the minimum value of any port is 1280 bytes

Command Mode

VLAN interface configuration mode

Usage Guidelines

When MTU is the default value, RA has the MTU option

When a switch forwards packet, a packet will not be fragmented just because the MTU of the egress is smaller than the packet's length. But it will be fragmented only when the transmitted packet is generated

Example

The following example shows how to set MTU of the interface:

Switch_config_v1# ipv6 mtu 1400

Related Command

show ipv6 interface

28.4 ipv6 redirects

Syntax

To control whether to transmit a redirection packet after the packet is forwarded, run **ipv6 redirects**

ipv6 redirects

no ipv6 redirects

Parameter

None

Default

The redirection packet will be transmitted by default

Command Mode

VLAN Interface configuration mode

Usage Guidelines

The redirection packets are transmitted through the ICMPv6 protocol

Example

1.The following example shows how to enable a port to transmit the redirection packet

Switch_config_v1# ipv6 redirects

2.The following example shows how to disable a port to transmit the redirection packet

Switch_config_v1# no ipv6 redirects

Use **show ipv6 interface** command can check whether the port will transmit the redirection packet

Related Commands

show ipv6 interface

28.5 ipv6 access-group

Syntax

To filter the received packet of some port, run the first one of the following commands. To return to the default setting, use the no form of this command.

ipv6 access-group access-list-name { in | out }

no ipv6 access-group { in | out }

Parameter

Parameter	Description
access-list-name	access list name
In	Filter direction, receiving packets
Out	Filter direction, forwarding packets

Default

The filter function is not set by default

Command Mode

VLAN interface configuration

Usage Guidelines

None

Example

The following example shows how to use the access list test to filter packets when received in port vlan 1:

Switch_config_v1# ipv6 access-group test in

Related Commands

Ipv6 access-list

Show ipv6 interface

28.6 ipv6 unreachables

Syntax

To enable an interface to generate and transmit the ICMPv6 unreachable packets, run **ipv6 unreachable**

ipv6 unreachables

no ipv6 unreachables

Parameter

None

Default

The unreachable packets are transmitted by default

Command Mode

VLAN Interface configuration mode

Usage Guidelines

The unreachable packets are transmitted through the ICMPv6 protocol

Example

The following example shows how to disable the VLAN interface to transmit the unreachable packets.

Switch_config_v1# no ipv6 unreachables

Related Commands

None

28.7 ipv6 route default

Syntax

To configure the default ip6 gateway, use ipv6 route default command.

ipv6 route default [NULL | X:X:X:X::X]

no ipv6 route default [NULL | X:X:X:X::X]

Parameter

Parameter	Description
NULL	NULL interface
X:X:X:X::X	**Gateway address**

Default

None

Command Mode

Global configuration mode

Example

The following example shows how to set the address of 2008::1 as the route default of the switch

ipv6 route default 2008::1

Related Command

None

28.8 show ipv6 general-prefix

Syntax

To display the detailed information about the general prefix of IPv6, run the following command:

show ipv6 general-prefix

Parameter

None

Command Mode

EXEC

Example

Switch_config#show ipv6 general-prefix

IPv6 Prefix my-prefix, acquired via manual

2002::/64

Vlan1 (Address command)

Field	Remarks
IPv6 Prefix	Stands for the name of the general IPv6 prefix defined by user
Acquire via	Stands for the configuration method of the general prefix. At present, the manual configuration and the automatic DHCP obtainment are supporte
Vlan1 (Address command)	Stands for a list of ports that use this general prefix

Related Commands

ipv6 general-prefix

28.9 show ipv6 pmtu

Syntax

To display the cache options of path MTU, run the following command:

show ipv6 pmtu

Parameter

None

Command Mode

EXEC

Example

Switch_config#show ipv6 pmtu

PMTU Expired Destination Address

1300 00:04:00 2002:1::1

1280 00:01:00 2001:2::2

The cache of path MTU stores the path MTU which is applied to reach a destination address. If the to-be-transmitted packets generated by routers or switches are bigger than the path MTU, they will be fragmented during being transmitted

The switch will create a path MTU record when receiving an ICMPv6 too-big packet

Field	Remarks
MTU	Stands for the value of the path MTU. It is this MTU that is contained in the received ICMPv6 too-big packet
Expired	It means expiration. The expiration time starts counting when the ICMPv6 "too-big" packet is received. When the **expired** parameter is 0, this path MTU record will be deleted
Destination Address	Stands for the destination address. It is this destination address that is contained in the received ICMPv6 too-big packet

Related Commands

ipv6 mtu

28.10 show ipv6 traffic

Syntax

To display the statistics of IPv6 flow, run the following command:

show ipv6 traffic

Parameter

None

Command Mode

EXEC

Example

```
Switch#show ipv6 traffic
IPv6 statistics:
  Rcvd: 0 total, 0 local destination
  0 badhdrs, 0 badvers
  0 tooshort, 0 toosmall, 0 toomanyhdrs
  0 source-routed, 0 badscope
  0 badopts, 0 unknowopts, 0 exthdrtoolong
  0 fragments, 0 total reassembled
  0 reassembly timeouts, 0 reassembly failures
  Sent: 25 generated, 0 forwarded, 0 cant forwarded
  0 fragmented into 0 fragments, 0 failed
  0 no route
  Mcast: 0 received, 25 sent
ICMP statistics:
  Rcvd: 25 total, 0 format errors, 0 checksum errors
  0 unreachable, 0 packet too big
  0 time exceeded, 0 parameter problem
  0 echos, 0 echo replies
  0 membership query, 0 membership report, 0 membership reduction
  0 Switch solicitations, 0 Switch advertisements
  0 neighbor solicitations, 0 neighbor advertisements, 0 redirect
  Sent: 0 total, 0 bandwidth limit
  0 unreachable, 0 packet too big
  0 time exceeded, 0 parameter problem
  0 echos, 0 echo replies
  0 membership query, 0 membership report, 0 membership reduction
  0 Switch solicitations, 0 Switch advertisements
```

0 neighbor solicitations, 0 neighbor advertisements, 0 redirect

Related Commands

clear ipv6 traffic

28.11 Network Test Tools Commands

IPv6 network test tools commands include:

ping6

traceroute6

28.11.1 ping6

Syntax

To test the accessibility and connectivity of the host, run the following command. The command enables the host forwards ICMP packets to another host and get ICMP response packets from it.

ping6 host [-a] [-l length] [-n number] [-v] [–w waittime] [-b internal]

Parameter

Parameter	Description
host	Destination host address or host name
-a	Continuous forward icmp echo request packets until the user disable it manually
-l *length*	Set the length of the ICMO data in the packets. The default is 56 bytes
-n *number*	Set the number of toal transmitted packets. The default one is 5 packets
-w *waittime*	The time of waiting each packet response. The default one is 2 seconds
-b *interval*	Set the time interval of transmitting ping packets Unit: 10ms; value ranges: 0-65535; the default is 0

Command Mode

Exec, global configuration mode

Usage Guidelines

To disable ping, press "q" or "Q"

The output by default:

Parameter	Description
!	Receive the response packet
.	No response packet in timeout
U	Receive the ICMP destination unreachable packet
R	Receive the ICMP redirection packet
T	Receive the ICMP timeout packet
P	Receive the ICMP parameter packet

The output of statistics information:

Parameter	Description
packets transmitted	The number of transmitted packets
packets received	The number of received packets, not include other ICMP packets
packet loss	The proportion of packet loss
round-trip min/avg/max	The minimum/average/max response time (ms)

The routing switch supports the destination address is the link-local address or multicast address. When ping this address, the command must designate the vlan interface first and forward ICMP echo packets on the interface. The routing switch will output all addresses of response hosts

Example

switch#ping6 2008::2 -l 10000 -n 30

PING 2008::2 (2008::2): 10000 data bytes

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

--- 2008::2 ping6 statistics ---

30 packets transmitted, 30 packets received, 0% packet loss

round-trip min/avg/max = 0/1/20 ms

·ping multicast address:

switch#ping6 ff02::1 vlan 1 -n 2

PING 1 (FF02:1B::1): 56 data bytes

Reply to request 0 from FE80::2E0:FFF:FEDB:583F, <10 ms

Reply to request 0 from FE80::1EAF:F7FF:FE35:D02A, 10 ms

Reply to request 1 from FE80::2E0:FFF:FEDB:583F, <10 ms

Reply to request 1 from FE80::1EAF:F7FF:FE35:D02A, 10 ms

28.12 traceroute6

The command is used to trace the destination route

Transmit the UDP packets (or ICMP ECHO packets) with different TTL (Time to Live) to the destination, so that the route of the destination can be traced. Each router in the path has to reduce its TTL by 1 at least before transmitting the ICMP response packets, therefore, TTL is an effective way for accounting. When the TTL of the packet reduce to 0, the router sends back ICMP timeout information to the source system. Transmit first response packet whose TTL is 1 and add 1 to the TTL in subsequent transmission until the receive the response packet or reach the max TTL value

Trace the router by detecting ICMP Time Exceeded information it sends back. When reaching the destination, the destination node can only sends back ICMP information that the port is unreachable, as traceroute transmit UDP packets whose port number is greater than 30000. The destination is arrived as the report is received

Syntax

traceroute6 host [-i source-ip-address] [-p port-number] [-q probe-count] [-t ttl] [-w waittime] [-x icmp]

Parameter

Parameter	Description
host	Destination host address or host name
-i *source-ip-address*	Sets the source IP address
-p *port-number*]	Sets the destination port number transmitting UDP packets. The default is 33434
-q *probe-count*	Sets the packet number of each detection. The default is 3 packets
-t *ttl*	Sets the IP TTL of the packet to ttl. The TTL is 1 in minimum by default and 30 in maximum
-w *waittime*	The time of each packet for waiting response. The default time is 3 seconds
-x icmp	Sets the detection packet as the ICMP ECHO packet. The default is UDP packet

Command Mode

EXEC, Global Configuration Mode

Usage Guidelines

The command is used to trace the router by UDP packets. To trace the router by ICMP ECHO packets by command –x icmp. To disable traceroute, press "q" or "Q"

Output by default:

Parameter	Description
!N	Receive ICMP destination unreachable packets (the route is unreachable, code: 0)
!P	Receive ICMP destination unreachable packets (forbid out of management, code: 1)
!S	Receive ICMP destination unreachable packets (not neighbor, code: 2)
!A	Receive ICMP destination unreachable packets (unreachable address, code: 3)
!	Receive ICMP destination unreachable packets (unreachable port, code: 4)

The output of statistics information:

Parameter	Description
hops max	Max trace hop number (The uplimit of ICMP increment)
byte datalen	Size of each trace packet

Example

switch#traceroute6 2008::2

tracert6 to 2008::2 , 30 hops max, 12 byte datalen

1 2008::2 0 ms * 0 ms

Chapter 29 Layer-2 Tunneling Protocol Configuration Commands

29.1 l2protocol-tunnel

Syntax

[no] l2protocol-tunnel [stp]

To set layer 2 protocol tunnel, run the above command

Parameter

None

Default

By default, the tunnel function of any L2 protocol is not enabled on the port of the switch

When the tunnel function is enabled, the tunnel function of all supported L2 protocols is enabled if no specific L2 protocol is designated

Usage Guidelines

Currently only STP supports the tunnel function in our switches

Example

The following example shows how to enable the tunnel function of the STP (include STP/PVST) on interface g0/2

Switch_config# interface g0/2
Switch_config_g0/2# l2protocol-tunnel stp

29.2 no spanning-tree

Syntax

no spanning-tree

To disable the STP of a port, run the above-mentioned command

Parameter

None

Default

STP can be enabled on all switch's ports by default

Usage Guidelines

This command is used to disable STP on the port of a tunnel entrance, preventing this port from influencing the devices that access the tunnel by sending the STP packets

Example

The following example shows how to disable STP on port g0/2:

```
Switch_config# interface g0/2
Switch_config_g0/2# no spanning-tree
```

Chapter 30 LLDP Configuration Commands

30.1 LLDP Commands

30.1.1 lldp run

Syntax

lldp run

no lldp run

To start up LLDP, run **lldp run**; to Disable LLDP, run **no lldp run**

Parameter

None

Default

Disabled

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following command is used to start up LLDP.

Switch_config# lldp run

30.1.2 lldp holdtime

Syntax

lldp holdtime *time*

no lldp holdtime

To configure the ttl value of LLDP, run **lldp holdtime *time***. To resume the default transmission delay, run **no lldp holdtime**

Parameter

Parameter	Description
time	Storage time of the transmitted message, ranging between zero to 65535 seconds

Default

120s

Usage Guidelines

In normal, the remote information stored in the MIB will be updated before its aging. But the update frame may be lost during the transmission process, causing the information in the MIB to age. To prevent this, set the TTL value so that it updates the LLDP frame multiple times during the aging time

Command Mode

Global configuration mode

Example

The following example shows how to set the ttl value of LLDP to 100 seconds.

Switch_config# lldp holdtime 100

Switch_config#

30.1.3 lldp timer

Syntax

lldp timer *time*

no lldp timer

To configure the transmission interval of LLDP, run **lldp timer time**. To resume the default transmission delay, run **no lldptimer**.

Parameter

Parameter	Description
time	Interval for transmitting the LLDP message, ranging between 5 to 65534 seconds

Default

30s

Usage Guidelines

The transmission interval of the LLDP message must be shorter than its storage time, ensuring multiple updates in the storage time and preventing error which is led by packet loss

Command Mode

Global configuration mode

Example

The following example shows how to configure the transmission interval of LLDP to 24 seconds

```
Switch_config# lldp  timer  24
Switch_config#
```

30.1.4 lldp reinit

Syntax

lldp reinit *time*

no lldp reinit

To configure the transmission delay of LLDP, run **lldp reinit time**. To resume the default transmission delay, run **no lldp reinit**

Parameter

Parameter	Description
time	Transmission delay of LLDP, whose values range from two to five seconds

Default

2s

Usage Guidelines

LLDP information is automatically sent when the status or value of one or more information elements (managed objects) in the local system changes and the transmission timer expires. Since a single information change requires sending LLDP packets, a series of continuous information changes may trigger the transmission of many LLDP frames. Only one change is reported in each frame. To avoid this situation, network management defines waiting time between two consecutively senting LLDP frames

Command Mode

Global configuration mode

Example

The following example shows how to set the transmission delay of LLDP to five seconds

```
Switch_config# lldp  reinit  5

Switch_config#
```

30.1.5 lldp tlv-select

Syntax

lldp tlv-select *tlv-type*

no lldp tlv-select *tlv-type*

To add TLV which is transmitted by the LLDP message, run **lldp tlv-select** ***tlv-type***. To delete TLV which is transmitted by the LLDP message, run **no lldp tlv-select** ***tlv-type***

Parameter

Parameter	Description
tlv-type	TLV that can be sent or not whose values are: management-address management address TLV port-description , port description TLV system-capabilities system capabilities TLV system-description, system description TLV system-name system name TLV

Default

All TLVs are sent

Usage Guidelines

Three mandatory TLVs must be sent

Command Mode

Global configuration mode

Example

The following example shows how to enable the port description not to be transmitted in the message

Switch_config#no lldp tlv-select port-description

Switch_config#

30.1.6 lldp dot1-tlv-select

Syntax

lldp dot1-tlv-select *tlv-type*

no lldp dot1-tlv-select *tlv-type*

To add TLV which is transmitted by the LLDP message, run **lldp dot1-tlv-select** *tlv-type*. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
tlv-type	Stands for TLV that are available for selective transmission. The value is: port-vlan-idport vlan address TLV protocol-vlan-idport and protocol VLAN ID TLV vlan-namevlan name TLV protocol-identity Protocol-identity TLV

Default

All TLVs are sent

Usage Guidelines

The TLV of the protocol identity does not support transmission but supports reception

Command Mode

Port Configuration Mode

Example

The following example shows how to enable the TLV not to be transmitted by deletion of the VLAN address of a port in the transmitted packet.

switch_config#int g0/1

switch_config_g0/1#no lldp dot1-tlv-select port-vlan-id

switch_config_g0/1#

30.1.7 lldp dot3-tlv-select

Syntax

lldp dot3-tlv-select *tlv-type*

no lldp dot3-tlv-select *tlv-type*

To add TLV which is transmitted by the LLDP message, run **lldp dot3-tlv-select** *tlv-type*. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
tlv-type	Stands for TLV that are available for selective transmission. The value is: link-aggregationlink aggregation TLV

macphy-confgMAC/Phy configuration/status TLV

max-frame-sizemax frame size TLV

powerPower Via MDI TLV

Default

All TLVs are sent

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following example shows how to enable the TLV not to be transmitted by deletion of the MAC/Phy configuration/status of a port in the transmitted packet

switch_config#int g0/1

switch_config_g0/1#no lldp dot3-tlv-select macphy-confg

switch_config_g0/1#

30.1.8 lldp med-tlv-select

Syntax

lldp med-tlv-select *tlv-type*

no lldp med-tlv-select *tlv-type*

To add TLV which is transmitted by the LLDP message, run lldp med-tlv-select tlv-type. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
tlv-type	Stands for TLV that are available for selective transmission. The value is: network-policynetwork policy TLV inventory detailed inventory management TLV locationLocation trace TLV power-managementExpand Power Via MDI TLV

Default

All TLVs are sent

Usage Guidelines

When the TLV of MED need be transmitted, the MED capability TLV must be transmitted. Hence it does not fall into the choice

Command Mode

Port Configuration Mode

Example

The following example shows how to enable the TLV not to be transmitted by deletion of the detailed list management in a transmitted packet

switch_config#int g0/1

switch_config_g0/1#no lldp med-tlv-select inventory

switch_config_g0/1#

30.1.9 lldp transmit

Syntax

lldp transmit

no lldp transmit

To set the port to send the LLDP message, run **lldp transmit**. To forbid receiving the LLDP message, run **no lldp transmit**

Parameter

None

Default

Transmittable LLDP message mode

Usage Guidelines

Only after the LLDP module is started can the command be valid

Command Mode

Port configuration mode

Example

The following example shows how to set port g0/1 not to send the LLDP message.

switch_config_g0/1# no lldp transmit
switch_config_g0/1#

30.1.10 lldp receive

Syntax

lldp receive

no lldp receive

To set the port to the receivable LLDP message mode, run **lldp receive**. To forbid receiving the LLDP message, run **no lldp receive**

Parameter

Default

Receivable LLDP message mode

Usage Guidelines

Only after the LLDP module is started can the configuration be valid

Command Mode

Port configuration mode

Example

The following example shows how to set port g0/1 to the LLDP message mode

```
switch_config_g0/1# no lldp receive
switch_config_g0/1#
```

30.1.11 lldp management-ip

Syntax

lldp management-ip *A.B.C.D*

no lldp management-ip

To configure the management address of the LLDP port, run **lldp management-ip A.B.C.D**. To resume the default transmission delay, run **no lldp management-ip**

Parameter

Parameter	Description
A.B.C.D	Stands for the management IP address that will be specified

Default

The default management address is the IP of vlan interface corresponding to pvid. If the IP is not existed, the default management address is 0.0.0.0

Usage Guidelines

The configured management IP address should be the IP address related with a port

Command Mode

Interface configuration mode

Example

The following example shows how to set the management IP address of the port g0/1 to 90.0.0.99:

switch_config_g0/1# lldp management-ip 90.0.0.99

switch_config_g0/1#

30.1.12 lldp trap-send

Syntax

lldp tranp-sendlldp-mib

To send trap notification to lldp mib base, run the above command

lldp tranp-sendptopo-mib

To send trap notification to ptopo mib base, run the above command

Parameter

None

Default

None

Usage Guidelines

None

Command Mode

Global Configuration mode

Example

The following example shows how to send trap notification to lldp mib base, run the following commands.

switch_config#lldp trap-send lldp-mib

switch_config#

The following example shows how to send trap notification to ptopo mib base, run the following command.

switch_config#lldp trap-send ptopo-mib

switch_config#

30.1.13 location elin identifier id WORD

Syntax

location elin identifier *id WORD*

no location elin identifier *id*

To add the elin information, run **location elin identifier id WORD**; to delete the elin information, run **no location elin identifier id**

Parameter

Parameter	Description
id	Stands for the ID of the to-be-set elin, which ranges from 1 to 65535
WORD	Stands for the content of the configured elin, which ranges from 10 to 25 bytes

Default

None

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to set the identifier to 1 and the content of elin to 1234567890.

switch_config# location elin identifier 1 1234567890

switch_config#

30.1.14 location civic identifier id

Syntax

location civic identifier *id*

no location civic identifier *id*

To enter the location configuration mode and set the civic information, run **location civic identifier id**. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
id	Stands for the ID of the to-be-set civic, which ranges from 1 to 65535

Default

None

Usage Guidelines

After the system enters the location configuration mode, you can run the following commands to conduct the corresponding configuration to the civic of the ID. To return to the default setting, use the no form of this command

Command	Purpose
(no) language WORD	Sets the language
(no) state WORD	Sets the state's (administrative district, district, province) name, such as shanghai
(no) county WORD	Sets the name of a county
(no) city WORD	Sets the name of a city
(no) division WORD	Sets the name of a division
(no) neighborhood WORD	Sets the name of neighborhood
(no) street WORD	Sets the name of a street
(no) leading-street-dir WORD	Sets the direction of a main street, such as N (north)
(no) trailing-street-suffix WORD	Sets the suffix of a small street, such as SW
(no) street-suffix WORD	Sets the suffix of a street, such as platz
(no) number WORD	Sets the street number, such as number 123
(no) street-number-suffix WORD	Sets the suffix of the street number, such as number 1/2 of A road
(no) landmark WORD	Sets the landmark, such as Colombia University
(no) additional-location WORD	Sets the additional location
(no) name WORD	Sets the information about a resident, such as Joe's haircut shop
(no) postal-code WORD	Sets the postal code
(no) building WORD	Sets the information about a building

(no) unit WORD	Sets the information about a unit
(no) floor WORD	Sets the information about a floor
(no) room WORD	Sets the information about a room
(no) type-of-place WORD	Sets the type of a place, such as office
(no) postal-community WORD	Sets the name of a postal office
(no) post-office-box WORD	Sets the name of a postal box, such as 12345
(no) additional-code WORD	Sets the additional code
(no) country WORD	Sets the name of a country
(no) script WORD	Sets the script

Command Mode

Global Configuration Mode

Example

The following example shows how to set the civic information of identifier 1

```
Switch_config#location civic identifier 1
Switch_config_civic#language English
Switch_config_civic#city Shanghai
Switch_config_civic#street Curie
Switch_config_civic#script EN
Switch_config_civic#quit
Switch_config#
```

30.1.15 location elin/civic id

Syntax

location elin/civic *id*

no location elin/civic

To set the location for a port, run **location elin/civic id**. To delete the location of a port, run **no location elin/civic**

Parameter

Parameter	Description
id	Stands for the ID of the to-be-set elin, which ranges from 1 to 65535

Default

None

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following example shows how to set the elin and the civic for a port.

Switch_config#int g0/8

Switch_config_g0/8#location elin 1

Switch_config_g0/8#location civic 1

30.1.16 show lldp errors

Syntax

Show lldp errors

It is used to display the error information about the LLDP module

Parameter

None

Default

None

Usage Guidelines

None

Command Mode

EXEC/Global configuration mode

Example

The following example shows how to view the error information of the lldp module.

```
switch_config#show lldp errors
LLDP errors/overflows:
Total memory allocation failures: 0
Total encapsulation failures: 0
Total table overflows: 0
switch_config#
```

30.1.17 show lldp interface

Syntax

Show lldp interface *interface-name*

To check the transmission and reception mode, run **show lldp interface interface name**

Parameter

Parameter	Description
interface-name	Name of the interface, such as g0/1 and GigaEthernet0/1

Default

None

Usage Guidelines

After LLDP is started, you can check the state of the port

Command Mode

EXEC/global configuration mode

Example

The following example shows how to check the transmission and reception mode of port g0/1

```
switch_config#show lldp interface g0/1
GigaEthernet0/1:
Rx: enabled
Tx: enabled
switch_config#
```

30.1.18 show lldp neighbors

Syntax

show lldp neighbors

It is used to display the simple information about neighbors

Parameter

None

Default

None

Usage Guidelines

The command is used to display the simple information about neighbors

Command Mode

EXEC / global configuration mode

Example

```
switch_config#show lldp neighbors
Capability Codes:
(R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone
(W)WLAN Access Point, (P)Repeater,(s)station,(O)Other

Device-ID       Local-Intf      Hldtme      Port-ID         Capability
switch          Gig0/2          115           Gig0/32         B
switch          Gig0/32         114           Gig0/2          B

Total entries dispalyed: 2
switch_config#
```

30.1.19 show lldp neighbors detail

Syntax

Show lldp neighbors detail

It is used to display the detailed information about the neighbor

Parameter

None

Default

None

Usage Guidelines

None

Command Mode

EXEC/global configuration mode

Example

```
switch_config#show lldp neighbors detail

chassis id: 00e0.0f61.ca53
port id: Gig0/32
port description: GigaEthernet0/32
system name: switch

system description: s3448 software, Version 2.0.1K
```

serial: s35000456
Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 98
system capabilities: R B
enabled capabilities: B
Managment Address:
IP: 192.168.213.62

Auto Negotiation -- supported,enabled
Physical media capabilitise:
100baseTX(FD)
100baseTX(HD)
10baseT(FD)
10baseT(HD)
Media Attachment Unit type: 16

---

chassis id: 00e0.0f61.ca35
port id: Gig0/2
port description: GigaEthernet0/2
system name: switch

system description: s3448 software, Version 2.0.1K
serial: s35000456
Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 95
system capabilities: R B
enabled capabilities: B
Managment Address:
IP: 90.0.0.66

Auto Negotiation -- supported,enabled
Physical media capabilitise:
100baseTX(FD)
100baseTX(HD)
10baseT(FD)
10baseT(HD)
Media Attachment Unit type: 16

Total entries dispalyed: 2
switch#

30.1.20 show lldp traffic

Syntax

Show lldp traffic

To display all statistics information about LLDP, run **show lldp traffic**

Parameter

None

Default

None

Usage Guidelines

None

Command Mode

EXEC/global configuration mode

Example

switch_config#show lldp traffic

LLDP traffic statistics:

Total frames out: 1599

Total entries aged: 0

Total frames in: 624

Total frames received in error: 0

Total frames discarded: 0

Total TLVs unrecognized: 0

switch_config#

30.1.21 show location elin

Syntax

show location elin

To display the elin configuration of the location, run the above command

Parameter

None

Default

None

Usage Guidelines

None

Command Mode

EXEC/Global Configuration Mode

Example

```
Switch_config#show location elin
elin information:
  elin 2: 0987654321
  elin 1: 1234567890
total: 2
Switch_config#
```

30.1.22 show location civic [identifier *id*]

Syntax

show location civic [identifier *id*]

To display the civic information of the location, run the above command

Parameter

Parameter	Description
id	Stands for the ID of the to-be-set civic, which ranges from 1 to 65535

Default

None

Usage Guidelines

None

Command Mode

Exec/ Global Configuration Mode

Example

```
Switch_config#show location civic
civic address information:
  identifier: 2
  Language: Chinese
  Script: CN
-------------------------------------
```

```
    identifier: 1
    City: Shanghai
    Language: English
    Script: EN
  ---------------------------------------
  total: 2
  Switch_config#
```

30.1.23 clear lldp counters

Syntax

clear lldp counters

To clear the statistics information, run **clear lldp counters**

Parameter

None

Default

None

Usage Guidelines

None

Command Mode

EXEC

Example

```
switch#clear lldp counters
 switch#
 switch#show lldp traffic
 LLDP traffic statistics:
      Total frames out: 0
      Total entries aged: 0
      Total frames in: 0
      Total frames received in error: 0
      Total frames discarded: 0
      Total TLVs unrecognized: 0
 switch#

switch#show lldp errors

LLDP errors/overflows:

      Total memory allocation failures: 0

      Total encapsulation failures: 0

      Total table overflows: 0

switch#
```

30.1.24 clear lldp table

Syntax

clear lldp table

To remove the neighbor list, run **clear lldp table**

Parameter

None

Default

None

Usage Guidelines

None

Command Mode

EXEC

Example

```
switch#clear lldp table
switch#
switch#show lldp neighbors
Capability Codes:
        (R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone
        (W)WLAN Access Point, (P)Repeater,(s)station,(O)Other

Device-ID       Local-Intf      Hldtme      Port-ID      Capability

Total entries displayed: 0
```

Chapter 31 Loopback Detection Configuration Commands

31.1 loopback-detection

Syntax

[no] loopback-detection

To enable or disable global loopback detection, run the above-mentioned command

Parameter

None

Default

Loopback detection is globally disabled by default

Command Mode

Global configuration mode

Usage Guidelines

None

Example

```
Switch#config
Switch_config#
Switch_config#loopback-detection
```

31.2 loopback-detection enable

Syntax

[**no**] **loopback-detection enable**

To enable or disable loopback detection on a port, run the above-mentioned command

Parameter

None

Default

Loopback detection is disabled on a port by default

Command Mode

Port configuration mode

Usage Guidelines

You can run this command to enable or disable loopback detection on a specified port. However, this settings takes effect only after loopback detection is enabled globally

Example

```
Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection enable
```

31.3 loopback-detection vlan-control

Syntax

[**no**] **loopback-detection vlan-control** *vlan-list*

To set a port to perform loopback detection toward a specified VLAN, run the above-mentioned command

Parameter

Parameter	Description
vlan-list	Stands for a VLAN specified by a port. It ranges from 1 to 4094, and up to 10 VLANs can be specified

Default

None

Command Mode

Port configuration mode

Usage Guidelines

After loopback detection is configured on a specified VLAN, the port transmits multiple detection packets of specified VLAN tag regularly and the number of these detection packets transmitted by this port can be up to 10

Example

Switch_config# **interface** *tg1/1*
Switch_config_tg1/1# **loopback-detection vlan-control** *1-5*

31.3.1 loopback-detection hello-time

Syntax

[**no**] **loopback-detection hello-time** *hello-time*

To set the transmission period of loopback detection packets, run the above-mentioned command

Parameter

Parameter	Description

hello-time	Stands for the transmission period of loopback packets, whose unit is second

Default

3 seconds

Command Mode

Port configuration mode

Usage Guidelines

None

Example

None

31.3.2 loopback-detection recovery-time

Syntax

[**no**] **loopback-detection recovery-time** *recovery-time*

To set the recovery time of a port after being controlled, run the above-mentioned command

Parameter

Parameter	Description
recovery-time	Stands for the recovery time of a port after being controlled, whose unit is second

Default

10 seconds

Command Mode

Port configuration mode

Usage Guidelines

None

Example

None

31.3.3 loopback-detection delay-time

Syntax

[**no**] **loopback-detection delay-time** ***delay-time***

Configure the time period for delaying the execution of controlled actions after the port detects a loop

Parameter

Parameter	Description
delay-time	The delay time for execution of controlled actions after the port detects a loop. Unit: seconds

Default

0s

Command Mode

Port configuration mode

Usage Guidelines

None

Example

None

31.3.4 loopback-detection control

Syntax

[no] **loopback-detection control { block|learning|shutdown|isolate-vlan}**

To set a port to be controlled, run the above-mentioned command

Parameter

Parameter	Description
block	Sets a port to be blocked
learning	Sets a port to be learning
shutdown	Sets a port to be shutdown
isolate-vlan	Configures the port as isolate-vlan

Default

None

Command Mode

Port configuration mode

Usage Guidelines

When a port detects loopback exists in its network, you can perform corresponding control actions to this port by setting control functions. The controlled states of a port include block, nolearn, shutdown and trap. When a controlled state is configured and loopback exists on a port, the trap message can be transmitted. The trap is configured by default

After loopback detection is enabled globally, the port on which loopback detection is enabled transmits the loopback detection packets and receives the already transmitted loopback detection packets. Four control actions are conducted on the port:

block: This means to block the port. When loopback is found, this port will be isolated from other ports and the packets going into this port cannot be forwarded to other ports. This port is then in protocol down state and its MAC address table ages

learning: This means forbidding this port to learn MAC addresses.Upon the discovery of loopback on a port, this port will not learn MAC addresses and at the same time age its MAC address table

shutdown: It means to shut down the port. At the discovery of loopback, this port will not only transmit the trap message and age its MAC address but also shut down this port automatically to stop packet reception and transmission until the err-disable-recover time comes

Isolate-vlan: When multi-vlan loop detection is performed, if a vlan detects a loop, the vlan will be deleted from the vlan-allowed of the port, and the forwarding of data packets of this vlan is prohibited (the port needs to be configured in trunk mode).**trap:** It means that the port only reports alarms. When loopback is discovered, the port will only report alarms and age its MAC address table

When a port is blocked, the packets entering into this port cannot be forwarded by this port and this port will go on transmitting loopback detection packets at the same time; when loopback disappears, the port will recover itself automatically. Loopback disappearance takes place if the port has not received loopback detection packets within 10 seconds

In block state the port protocol is down, while in shutdown state the port's link is down directly

Example

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection control block
```

31.3.5 loopback-detection frames-threshold

Syntax

[no] loopback-detection frames-threshold *frames-threshold*

To configure the upper limit of loop detection frames received per second, run the above-mentioned command

Parameter

Parameter	Description
frames-threshold	The upper limit of loop detection frames received per second (10-200)

Default

None

Command mode

Port configuration mode

Usage Guidelines

To configure the upper limit of loop detection frames received every second on the designated port, please enable the loop detection function globally at first

Note: Loop detection is invalid for PON ports

Example

```
Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1# loopback-detection frames-threshold 20
```

31.3.6 loopback-detection frames-monitor

Syntax

[no] loopback-detection frames-monitor

To configure the port to enable or disable frames-monitor function, run the above-mentioned command

Parameter

None

Default

Disable the frame number detection function of this port

Command mode

Port configuration mode

Usage Guidelines

None

Example

```
Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection frames-monitor
```

31.3.7 loopback-detection dest-mac

Syntax

[**no**] **loopback-detection dest-mac** *mac-addr*

To set the destination MAC address of loopback detection packets on a port, run the above-mentioned command

Parameter

Parameter	Description
mac-addr	Stands for the destination MAC address of loopback detection packets

Default

The default destination MAC address is **01-80-C2-00-00-0a**

Command Mode

Port configuration mode

Usage Guidelines

None

Example

```
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection dest-mac 1111.1111.1111
```

31.3.8 loopback-detection existence

Syntax

[no] loopback-detection existence

To set a standard to judge whether loopback exists on a port when this port is enabled or its link state is UP, run the above-mentioned command

Parameter

None

Default

Loopback is nonexistent by default

Command Mode

Port configuration mode

Usage Guidelines

This command is mainly used to solve the problem that loopback exists on a port or not when this port is up and its loopback detection function takes effect. When the controlled action of this port is set to **shutdown**, it is improper to regard that loopback exists on this port for a shutdown port has already not forwarded packets

Example

None

31.3.9 loopback-detection forbid-packet

Syntax

[no] loopback-detection forbid-packet

Configure to prohibit forwarding of all loopback-detect packets on this port

Parameter

None

Default

Disabled

Command Mode

Port configuration mode

Usage Guidelines

This command is used to prohibit forwarding of all loopback-detect packets on this port

Example

None

31.3.10 loopback-detection vlan-recovery

Syntax

loopback-detection vlan-recovery

Restore the vlan where the port was isolated in isolate-vlan mode

Parameter

None

Default

Default is no configuration

Command Mode

Port configuration mode

Usage Guidelines

In the isolate-vlan mode, run this command to release the VLAN that is isolated due to the detection of a loop

Example

None

31.3.11 show loopback-detection

Syntax

show loopback-detection

To display the configuration details of loopback detection, run the above-mentioned command

Parameter

None

Default

None

Command Mode

EXEC, global or interface configuration modes

Usage Guidelines

This command is used to display the global or port's loopback detection configurations and port status

Example

Switch#show loopback-detection

Loopback-detection is enable

Interface state information

Port	Status	dest MacAddress	Control	VLAN
G0/1	UP	1234.5678.9abc	BLOCK	1-5
G0/2	UP	0180.c200.000a	WARNING	
G0/3	UP	0180.c200.000a	BLOCK	
G0/4	UP	0180.c200.000a	WARNING	
G0/5	UP	0180.c200.000a	WARNING	
G0/6	UP	0180.c200.000a	WARNING	1-8
G0/7	UP	0180.c200.000a	WARNING	
G0/8	UP	0180.c200.000a	WARNING	
G0/9	UP	0180.c200.000a	WARNING	
G0/10	UP	0180.c200.000a	WARNING	
G0/11	UP	0180.c200.000a	WARNING	
G0/12	UP	0180.c200.000a	WARNING	
G0/13	UP	0180.c200.000a	WARNING	
G0/14	UP	0180.c200.000a	WARNING	

G0/15 UP 0180.c200.000a WARNING

G0/16 UP 0180.c200.000a WARNING

31.3.12 show loopback-detection

Syntax

show loopback-detection *intf-id*

To display the information about the loopback detection port, run the above-mentioned command

Parameter

Parameter	Description
Interface *Intf-id*	Displays the designated port

Default

None

Command Mode

EXEC, global or interface configuration modes

Usage Guidelines

This command is mainly used to display the status of the loopback detection port

Example

Switch#show loopback-detection interface g0/1

Receive Packets :0

Transmit Packets: 20

Discard Packets:0

HelloTimeOut:10

RecoverTimeOut:26

Chapter 32 MAC Access List Configuration Commands

32.1 mac access-list

Syntax

To add a MAC access list, use the **mac access-list** command. To delete a MAC access list, use the **no mac access-list** command

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

Parameter

Parameter	Description
name	MAC access list name

Default

If there is any entry is configured, one **deny any any** will be added at the end by default, and it is not displayed

Command Mode

Global configuration mode

Example

The following example establishes MAC access list named mac-acl:

Switch-config# mac access-list mac-acl

Switch-config-macl#

32.2 permit

Syntax

To add a permit entry to the MAC access list, use the **permit** command. To delete a permit entry to the MAC access list, use the **no permit** command

[**no**] **permit** {**any** | **host** *src-mac-addr* / *src-mac-addr src-mac-mask* } {**any** | **host** *dst-mac-addr* / *dst-mac-addr dst-mac-mask*}[**arp** [{*any* / *src-ip-addr*} {*any* / *dst-ip-addr* }] | *ethertype* / *cos value*]

Parameter

Parameter	Description	Value range
any	Any value	-

host	Host	-
src-mac-addr	Source MAC address	H.H.H
src-mac-addr-mask	Source MAC address mask	H.H.H
dst-mac-addr	Destination MAC address	H.H.H
dst-mac-addr-mask	Destination MAC address mask	H.H.H
arp	Matched arp message	-
src-ip-addr	Source IP address	A.B.C.D
dst-ip-addr	Destination IP address	A.B.C.D
ethertype	Types of the matching ethernet data packet.	0x0600-0xFFFF
cos value	Header mark of message	0-7

Default

Deny all

Command Mode

MAC access list configuration mode

Example

The following example shows how to permit host whose source MAC address is 1234.5678.abcd:

Switch-config-macl#permit host 1234.5678.abcd any

32.3 deny

Syntax

To add/ delete a deny entry to the MAC access list, use the following command

[**no**] **deny** {**any** | **host** *src-mac-addr* / *src-mac-addr src-mac-mask* } {**any** | **host** *dst-mac-addr* / *dst-mac-addr dst-mac-mask*}[**arp** [{*any* / *src-ip-addr*} {*any* / *dst-ip-addr* }] | *ethertype* / *cos value*]

Parameter

Parameter	Description	Value range
any	Any value	-
host	Host	-

src-mac-addr	Source MAC address	H.H.H
src-mac-addr-mask	Source MAC address mask	H.H.H
dst-mac-addr	Destination MAC address	H.H.H
dst-mac-addr-mask	Destination MAC address mask	H.H.H
arp	Matched arp message	-
src-ip-addr	Source IP address	A.B.C.D
dst-ip-addr	Destination IP address	A.B.C.D
ethertype	Types of the matching ethernet data packet.	0x0600-0xFFFF
cos value	Header mark of message	0-7

Default

Deny all

Comamnd mode

MAC access list configuration mode

Example

The following example shows how to deny host whose source MAC address is 1234.5678.abcd:

Switch-config-macl#deny host 1234.5678.abcd any

32.4 mac access-group

Syntax

Apply the configured MAC access list in interface configuration mode or global configuration mode, or delete the MAC access list applied in interface configuration mode or global configuration mode

Global configuration mode:

mac access-group *name* **[vlan** {*word* **| add** *word* **| remove** *word*}**]**

[**no**] **mac access-group** *name* **[vlan]**

Interface configuration mode:

[**no**] **mac access-group** *name*

Parameter

Parameter	Description

name	Name of the MAC access list.
Vlan	The access list is applied to the inbound VLAN.
Word	VLAN range table
add	Add VLAN range table
remove	Remove VLAN range table

Default

No MAC access list is applied

Command Mode

Use the command in layer-2 global or interface configuration mode. If the access list does not exist, an access list with no rule will be created

Example

The following example shows how to configure MAC access list named macacl on interface g0/1:

Switch_config_g0/1#mac access-group macacl

Chapter 33 MAC Address Configuration Commands

33.1 mac address-table static

Syntax

To add/delete a static MAC address, use the **mac address-table static** command

[**no**] **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Parameters

Parameter	Description
mac-addr	MAC address. Value format: H.H.H.
vlan-id	Vlan id of the MAC address, in the range from 1 to 4094.
interface-id	Interface id of the MAC address.

Default

None

Command Mode

Global configuration mode

Example

The following example binds the MAC address 0004.5600.67ab to the interface g0/2 of VLAN 1:

Switch_config# mac address-table static 0004.5600.67ab vlan 1 interface g0/2

33.2 mac address-table aging-time

Syntax

To configure the maximum aging time for MAC address table

mac address-table aging-time [**0** | **10-1000000**]

Parameters

Parameter	Description
0	The aging time for MAC address table is disabled

10-1000000	The aging time (in seconds) for MAC address table

Default

300s

Command Mode

Global configuration mode

Example

The following example configures the aging time for MAC address table to 100 seconds:

Switch_config# mac address-table aging-time 100

33.3 mac address-table blackhole

Syntax

To add/ delete a blackhole MAC address

[**no**] **mac address-table blackhole***mac-addr* **vlan** *vlan-id*

Parameters

Parameter	Description
mac-addr	MAC address. Value format: H.H.H
vlan-id	VLAN ID, in the range from 1 to 4094

Default

None

Usage Guidelines

Global configuration mode

Example

The following example shows how to binds the MAC address 0004.5600.67ab to the mac blackhole of VLAN 1:

Switch_config# mac address-table blackhole 0004.5600.67ab vlan 1

33.4 show mac address-table

Syntax

To display the content of the switch MAC address table, use the **show mac address-table** command

show mac address-table [dynamic [interface *interface-id* | **vlan** *vlan-id***]** | **static | brief | multicast | interface** *interface-id* **| vlan** *vlan-id* **| H.H.H | blackhole]**

Parameters

Parameter	Description
dynamic	The dynamic MAC address table.
interface-id	Interface name
vlan-id	VLAN ID, in the range from 1 to 4094.
static	The static MAC address table.
brief	Brief information of Mac address
multicast	Multicast of mac address table
Interface	Interface of mac address table
Vlan	Mac address table in VLAN
H.H.H	Specific address
Blackhole	Blackhole of mac address table

Default

None

Usage Guidelines

The command is used to display MAC address table

Example

The following example displays all dynamic MAC address tables:

Switch_config#show mac address-table

Mac Address Table (Total 2)

Vlan	Mac Address	Type	Ports
----	----------	----	-----
1	0026.5a7c.fad3	DYNAMIC	g0/2

33.5 clear mac address-table

Syntax

To delete a dynamic MAC address, use the **clear mac address-table**

clear mac address-table dynamic [address *mac-addr* | interface *interface-id* | vlan *vlan-id*]

Parameter

Parameter	Description
mac-addr	The MAC address. Value range: H.H.H
interface-id	Layer 2 interface name
vlan-id	VLAN ID, in the range from 1 to 4094

Default

None

Command Mode

Use the command in the management mode

Example

The following example deletes all MAC addresses that acquire dynamically on interface g0/2:

Switch# clear mac address-table dynamic interface g0/2

Chapter 34 MACFF Configuration Commands

34.1 macff enable

Syntax

To enable or disable the MACFF function globally, run the following command. To return to the default setting, use the no form of this command

macff enable

no macff enable

Parameters

None

Default Value

MACFF function is disabled by default

Usage Guidelines

None

Example

The following example shows how to enable the MACFF function

Switch_config#macff enable

Switch_config#

34.2 macff vlan *vlan_id* enable

Syntax

macff vlan *vlan_id* **enable**

no macff vlan *vlan_id* **enable**

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

None

Usage Guidelines

The command is used to send MAC-Based VLAN

Example

The following example shows how to enable MACFF on VLAN 2 and the default gateway address is 192.168.1.1.

Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed vlan 2

Switch_config#macff vlan 2 enable
Switch_config#

34.3 macff vlan *vlan_id* default-ar *A.B.C.D*

Syntax

To bind DHCP snooping to standby TFTP server, run the following command. To return to the default setting, use the no form of this command

macff vlan *vlan_id* **default-ar** *A.B.C.D*

no macff vlan *vlan_id* **default-ar** *A.B.C.D*

Parameters

Parameters	Description
A.B.C.D	IP address of the default gateway

Default Value

None

Usage Guidelines

This command is used when you set the IP address of the client host and the default gateway manually. Of course, you also need to add the DHCP snooping binding table manually

Example

The following example shows how to set the address of MACFF binding gateway in vlan1 to 192.168.1.1 and the client's address to 192.168.1.10.

Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed vlan 1

Switch_config#ip source binding 6c:62:6d:59:18:b6 192.168.1.10 interface GigaEthernet0/1

Switch_config# macff vlan 1 default-ar 192.168.1.1
Switch_config#

34.4 macff vlan *vlan_id* enable other-ar *A.B.C.D*

Syntax

macff vlan *vlan_id* **other_ar** *A.B.C.D*

no macff vlan *vlan_id* **other_ar** *A.B.C.D*

Parameters

Parameters	Description
A.B.C.D	Stands for the IP address of service AR

Default Value

None

Usage Guidelines

When the network segment where the client host is has other service ARs and these ARs are only accessed by the client directly without the need of gateway to forwarding packets, this command can be used to add these service ARs

Example

The following example shows how to set an AR with its IP being 192.168.2.254 and its MAC being 00:e0:0f:23:02:fc on port g0/1 in vlan1

Switch_config#arp 192.168.2.254 00:e0:0f:23:02:fc vlan 1

Switch_config#interface g0/1

Switch_config_g0/1# dhcp snooping trust

Switch_config_g0/1#exit

Switch_config#macff vlan 1 other_ar 90.1.1.1

34.5 macff disable

Syntax

macff disable

no macff disable

Parameters

None

Default Value

A specified port is allowed to enable MACFF

Usage Guidelines

Though MACFF is enabled in a VLAN, MACFF can be disabled on one of the ports in this VLAN. The DHCPR snooping functionality is not affected on this port after disabled its MACFF functionality

Example

The following example shows how to disable MACFF on port g0/1

Switch_config_g0/1#macff disable

Switch_config_g0/1#

34.6 debug macff

Syntax

debug macff

no debug macff

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the MACFF debugging switch

Example

The following example shows how to enable the debugging switch of MACFF

Switch_config#debug macff

Switch_config#

Chapter 35 LACP MAD Configuration Commands

35.1 multi-active-detection

Syntax

To enable/disable LACP MAD, run the following command

[no] multi-active-detection

Parameter

None

Default

LACP MADis disabled

Usage Guidelines

None

Command Mode

Aggregate port configuration mode

Example

The following example shows how to enable the LACP MAD function on the aggregate port P1:

Switch_config#interface port-aggregator 1

Switch_config_p1#multi-active-detection

35.2 multi-active-relay

Syntax

To enable/disable LACP Multi-Active Relay, run the following command

[no] multi-active-relay

Parameter

None

Default

LACP Multi-Active Relay is disabled

Usage Guidelines

None

Command Mode

Aggregate port configuration mode

Example

The following example shows how to enable LACP Multi-Active Relay feunction on aggregate port P1:

Switch_config#interface port-aggregator 1

Switch_config_p1#multi-active-relay

Chapter 36 MEAPS Configuration Commands

36.1 Global Configuration Commands

36.1.1 mether-ring id1 domain id2

Syntax

To set an instance of ring and enter the node mode, run the following command:

mether-ring *id1* **domain** *id2*

To cancel an instance of ring, run the following command:

no mether-ring *id1* **domain** *id2*

Parameter

Parameter	Description
Id1	Stands for the node instance ID, which ranges from 0 to 7
Id2	Stands for the domain instance ID, which ranges from 0 to 3

Default

By default, the ring node is not configured

Command Mode

Global configuration mode

Usage Guidelines

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#

Related Command

None

36.1.2 master-node

Syntax

To configure an Ethernet ring as a master node, run the following command:

master-node

Parameter

None

Default

By default, the node type is not configured

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#master-node

S1_config_ring1#

Related Commands

transit-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

36.1.3 transit-node

Syntax

Configures the node type to be a transit node

transit-node

Parameter

None

Default

By default, the node type is not configured

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1# transit-node

S1_config_ring1#

Related Commands

master-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

36.1.4 edge-node

To set the node type to be an edge node, run the following command:

edge-node

Parameter

None

Default

By default, the node type is not configured

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1# edge-node

S1_config_ring1#

Related Commands

master-node

transit-node

assistant-node

major-ring

sub-ring

control-vlan

36.1.5 assistant-node

To set the node type to be an assistant edge node, run the following command:

assistant-node

Parameter

None

Default

By default, the node type is not configured

Command Mode

Node configuration mode

Usage Guidelines

1.A node can be set to be a master node, a transit node, an edge node or an assistant node

2.After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1# assistant-node

S1_config_ring1#

Related Commands

master-node

transit-node

edge-node

major-ring

sub-ring

control-vlan

36.1.6 major-ring

Syntax

To set the node ring's level to be the major ring node, run the following command:

major-ring

Parameter

None

Default

By default, the node ring's level is not configured

Command Mode

Node configuration mode

Usage Guidelines

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified

3. The edge node and the assistant node cannot be set to major ring

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1# transit-node

S1_config_ring1#major-ring

S1_config_ring1#

Related Commands

master-node

transit-node

edge-node

assistant-node

sub-ring

control-vlan

36.1.7 sub-ring

Syntax

To set the node ring's level to be the sub-ring node, run the following command:

sub-ring

Parameter

None

Default

By default, the node type is not configured

Command Mode

Node configuration mode

Usage Guidelines

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified

3. If the edge node or the assistant node is set, they are regarded as sub-rings by default. Of course, you can set them not to be sub-rings

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#master-node

S1_config_ring1#sub-ring

S1_config_ring1#

Related Commands

master-node

transit-node

edge-node

assistant-node

major-ring

control-vlan

36.1.8 control-vlan

Syntax

To set the control VLAN of the ring node, run the following command:

control-vlan *vlan-id*

Parameter

Parameter	Description
vlan-id	ID of the control VLAN Value range: 1-4094

Default

By default, the control VLAN of a node is not configured

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. You can set any VLAN to be the control VLAN of a node and at the same time the system will create the corresponding system VLAN and another control VLAN according to the ring level

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the ring control VLAN can never be modified

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#master-node

S1_config_ring1#sub-ring

S1_config_ring1#control-vlan 2

S1_config_ring1#

Related Commands

master-node

transit-node

edge-node

assistant-node

major-ring

sub-ring

36.1.9 single-subring-mode

Syntax

To configure the edge node (assistant edge node) in the single-subring mode, use this command

single-subring-mode

Parameter

None

Default

By default, the single-subring mode is not configured

Command mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1.Configuration in single-subring mode can only be valid in the edge node (assistant edge node)

2.In single-subring mode, there is no state check for message channel of subring protocol on the main ring. Therefore, ensure no double-belong network group in the ring network

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#edge-node

S1_config_ring1#control-vlan 2

S1_config_ring1#single-subring-mode

Related Commands

None

36.1.10 hello-time

Syntax

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

hello-time *value*

To resume the default value of the cycle, run the following command:

no hello-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second The default value is three seconds. The value ranges between 1 and 10 seconds

Default

By default, the hello-time is three seconds

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The hello-time configuration validates only on the master node

2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked. After the hello-time is modified, the corresponding fail-time need be modified too

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#master-node

S1_config_ring1#sub-ring

S1_config_ring1#control-vlan 2

S1_config_ring1#hello-time 4

Related Command

fail-time

36.1.11 fail-time

Syntax

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

fail-time *value*

To resume the default value of the fail-time, run the following command:

no fail-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second The default value is three seconds. The value ranges between 3 and 30 seconds

Default

By default, the fail-time is 9 seconds

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The fail-time configuration validates only on the master node

2. By default, the value of the fail-time is triple of the fail-time, which avoids the Ethernet ring protocol from being shocked. After the hello-time is modified, the corresponding fail-time need be modified too

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#master-node

S1_config_ring1#sub-ring

S1_config_ring1#control-vlan 2

S1_config_ring1#hello-time 4

S1_config_ring1#fail-time 12

Related Command

hello-time

36.1.12 pre-forward-time

Syntax

Configures the time of maintaining the pre-forward state on the transit port

pre-forward-time *value*

To resume the default value of the pre-forward-time, run the following command:

no pre-forward-time

Parameter

Parameter	Description
value	Stands for a time value, whose unit is second The default value is three seconds. The value ranges between 3 and 30 seconds

Default

By default, the pre-forward-time is 9 seconds

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The pre-forward-time configuration validates only on the transit node

2. By default, the pre-forward-time on the transit node is three times the value of the hello-time on the master node, which avoids the network loop from being occurred after the transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node need be adjusted

Example

S1_config#mether-ring 1 domain 2

S1_config_ring1#transit-node

S1_config_ring1#sub-ring

S1_config_ring1#control-vlan 2

S1_config_ring1#pre-forward-time 12

Related Command

None

36.2 Port Configuration Commands

36.2.1 mether-ring *id1* domain *id2* primary-port

Syntax

To set a port to be the primary port of a master node, run the following command:

mether-ring *id1* **domain** *id2* **primary-port**

To cancel the primary port configuration of a port, run the following command:

no mether-ring *id1* **domain** *id2* **primary-port**

Parameter

Parameter	Description
Id1	ID of the node instance
Id2	ID of domain instance

Default

The primary port is not configured by default

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted

Example

S1_config#interface GigaEthernet 0/1

S1_config_g0/1# mether-ring 1 domain 2 primary-port

S1_config_g0/1#exit

Related Commands

master-node

mether-ring id1 domain id2 secondary-port

36.2.2 mether-ring id1 domain id2 secondary-port

Syntax

To set a port to be the secondary port of a master node, run the following command:

mether-ring *id1* **domain** *id2* **secondary-port**

To cancel the secondary port configuration, run the following command:

no mether-ring *id1* **domain** *id2* **secondary-port**

Parameter

Parameter	Description
Id1	ID of the node instance
Id2	ID of domain instance

Default

The secondary port on the master node is not configured by default

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The secondary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted

Example

S1_config#interface GigaEthernet 0/3

S1_config_g0/3# mether-ring 1 domain 2 secondary-port

S1_config_g0/3#exit

Related Commands

master-node

mether-ring id1 domain id2 primary-port

36.2.3 mether-ring id1 domain id2 transit-port

Syntax

To set a port to be the transit port of a transit node, run the following command:

mether-ring *id1* **domain** *id2* **transit-port**

To cancel the transit port, run the following command:

no mether-ring *id1* **domain** *id2* **transit-port**

Parameter

Parameter	Description
Id1	ID of the node instance

Id2	ID of domain instance

Default

The transit port on the transit node is not configured by default

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the transit node. Two transit ports can be configured on one transit node

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted

Example

S1_config_ring1#exit

S1_config#interface GigaEthernet 0/1

S1_config_g0/1# mether-ring 1 domain 2 transit-port

S1_config_g0/1#exit

S1_config#interface GigaEthernet 0/3

S1_config_g0/3# mether-ring 1 domain 2 transit-port

S1_config_g0/3#exit

Related Command

transit-node

36.2.4 mether-ring id1 domain id2 common-port

Syntax

To set a port to be a public port of an edge node (assistant edge node), run the following command:

mether-ring *id1* **domain** *id2* **common-port**

To cancel the public port, run the following command:

no mether-ring *id1* **domain** *id2* **common-port**

Parameter

Parameter	Description
Id1	ID of the node instance
Id2	ID of domain instance

Default

By default, there is no configuration of the public port of an edge node

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The public port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted

Example

S1_config_ring1#exit

S1_config#interface GigaEthernet 0/1

S1_config_g0/1# mether-ring 2 domain 2 common-port

S1_config_g0/1#exit

Related Command

edge-node

assistant-node

mether-ring id1 domain id2 edge-port

36.2.5 mether-ring id1 domain id2 edge-port

Syntax

To set a port to be an edge port of an edge node (assistant edge node), run the following command:

mether-ring *id1* **domain** *id2* **edge-port**

To cancel the edge port configuration of a port, run the following command:

no mether-ring *id1* **domain** *id2* **edge-port**

Parameter

Parameter	Description
Id1	ID of the node instance
Id2	ID of domain instance

Default

By default, there is no configuration of the edge port of an edge node

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The edge port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted

Example

S1_config_ring1#exit

S1_config#interface GigaEthernet 0/3

S1_config_g0/3# mether-ring 2 domain 2 edge-port

S1_config_g0/3#exit

Related Commands

edge-node

assistant-node

mether-ring id1 domain id2 common-port

36.3 Show Configuration Commands

36.3.1 show mether-ring

Syntax

To display the summary information about the Ethernet-ring node, run the following command:

show mether-ring *id1* **domain** *id2*

To display the detailed information about the Ethernet-ring node, run the following command:

show mether-ring *id1* **domain** *id2* **detail**

To display the information about the Ethernet-ring port, run the following command:

show mether-ring *id1* **domain** *id2* **interface** *intf-name*

To display the summary information about the Ethernet-ring node, run the following command:

show mether-ring

Parameter

Parameter	Description
Id1	ID of the node instance
Id2	ID of domain instance
intf-name	Name of an interface

Default

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

If the configured domain is 0, that is, id2 is o, domain id2 can be omitted

Example

None

Related Command

None

Chapter 37 MLD Multicast Configuration Commands

37.1 ipv6 mld-snooping

Syntax

ipv6 mld-snooping

no ipv6 mld-snooping

To enable MLD snooping, run **ipv6 mld-snooping**. To disable the MLD snooping, use the no form of the command

Parameter

None

Default

This command is used to enable MLD snooping

Usage Guidelines

After MLD snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the MLD-snooping), all multicast packets whose destination addresses are not registered on any port will be dropped

Example

The following example shows how to enable the MLD snooping function:

switch_config# ipv6 mld-snooping

37.2 ipv6 mld-snooping solicitation

Syntax

ipv6 mld-snooping solicitation

no ipv6 mld-snooping solicitation

To enable or disable the hardware forwarding of the multicast group, run **ip mld-snooping solicitation**.To resume the default value, run **no ip mld-snooping solicitation**

Parameter

None

Default

This function is shut down

Usage Guidelines

None

Example

The following example shows how to enable the hardware forward of the multicast group

switch_config#ipv6 mld-snooping solicitation

37.3 ipv6 mld-snooping vlan vlan_id static X:X:X:X::X interface intf_name

Syntax

ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*

no ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
X:X:X:X::X	IP address of the multicast
inft	An interface

Default

None

Usage Guidelines

This command is used to configure the static multicast address of VLAN. Its negative form is used to cancel the static multicast address

Example

The following example shows how to add the static multicast address, ff12::5, to interface g1/1

switch_config# ipv6 mld-snooping vlan 1 static ff12::5 interface g0/1

switch_config#

37.4 ipv6 mld-snooping timer router-age *timer_value*

Syntax

ipv6 mld-snooping timer router-age *timer_value*

no ipv6 mld-snooping timer router-age

Parameter

Parameter	Description
time value	Queries the time of the timer. Value range: 10-2147483647

Default

260 seconds

Usage Guidelines

This command is used to query the time of the timer of MLD-Snooping. The negative form of this command is used to resume the default value

Example

The following example shows how to set the query time of the router to 300 seconds.

switch_config# ipv6 mld-snooping timer router-age 300

switch_config#

37.5 ipv6 mld-snooping timer response-time *timer_value*

Syntax

ipv6 mld-snooping timer response-time *timer_value*

no ipv6 mld-snooping timer response-time

To configure the maximum response time of IGMP snooping, run **ip mld-snooping timer response-time** ***timer_value***. To resume the default value of IGMP snooping, run **no ip mld-snooping timer response-time** ***timer_value***.

Parameter

Parameter	Description
time value	Queries the time of the timer. Value range: 10-2147483647

Default

15 seconds

Usage Guidelines

None

Example

The following example shows how to set the query response time of IGMP snooping to 20 seconds

switch_config# ipv6 **mld-snooping** timer response-time 20

37.6 ipv6 mld-snooping querier

Syntax

Ipv6 mld-snooping querier [address *<ip_addr>***]**

no ipv6 mld-snooping querier [address]

To activate mld-snooping querier mechanism or set the source IP address of the query packet, run the first one of the above commands

To return to the default setting, use the no form of this command

Parameter

Parameter	Description
ip_addr	Normal unicast IPv6 address

Default

Querier function is not disabled. The default source IP address is FE80::3FF:FEFE:FD00:1

Usage Guidelines

None

Example

The following example shows how to activate IGMP querier and replace its work in condition of no multicast router.

switch_config# ipv6 mld-snooping querier

switch_config#

37.7 ipv6 mld-snooping vlan *vlan_id* mrouter interface *inft_name*

Syntax

ipv6 mld-snooping vlan *vlan_id* **mrouter** interface *inft_name*

no ipv6 mld-snooping vlan *vlan_id* **mrouter** interface *inft_name*

To set the static multicast router's port of MLD snooping, run the first one of the above-mentioned commands

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
inft_name	Shows the port type, the slot and the port ID

Default

None

Usage Guidelines

None

Example

The following example shows how to set interface G0/4 to be the interface of the static multicast router of MLD snooping.

switch_config# ipv6 mld-snooping vlan 1 mrouter interface g0/4

37.8 ipv6 mld-snooping vlan *vlan_id* immediate-leave

Syntax

ipv6 mld-snooping vlan *vlan_id* **immediate-leave**

no ipv6 mld-snooping vlan *vlan_id* **immediate-leave**

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default

The immediate-leave functionality is disabled

Usage Guidelines

This command is used to set the immediate-leave functionality

Example

The following example shows how to enable the immediate-leave functionality on VLAN 1:

switch_config# ipv6 mld-snooping vlan 1 immediate-leave

switch_config#

37.9 show ipv6 mld-snooping

Syntax

show ipv6 mld-snooping

Parameter

None

Default

None

Usage Guidelines

This command is used to display the information about MLD-snooping configuration

Example

The following example shows how to display the information about MLD snooping

switch#**show ipv6 mld-snooping**

```
Global MLD snooping configuration:
------------------------------------
Globally enable          : Enabled
Querier                  : Enabled
Querier address          : FE80::3FF:FEFE:FD00:1
Router age               : 260 s
Response time            : 10 s
Handle Solicitation    : Enabled

Vlan 1:
----------
      Running
      Routers: SWITCH(querier);
Vlan 2:
----------
      Running
      Routers: SWITCH(querier);
Switch_config#show ipv6 mld-s g
Vlan Group                Type Port(s)
---- --------------- ---- -------------------------------------
    1 FF02::1:FF13:647D MLD    G0/2
    1 FF02::1:FF13:394 MLD    G0/2
    2 FF02::1:FF00:2    MLD    G0/1
    1 FF02::1:FF00:12 MLD    G0/1
```

```
    1 FF02::1:FF00:2    MLD    G0/1
    2 FF02::1:FF61:9901 MLD    G0/2
switch#
```

37.10 show ipv6 mld-snooping vlan vlan_id

Syntax

show ipv6 mld-snooping vlan *vlan_id*

Parameter

Parameter	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default

None

Usage Guidelines

This command is used to display the concrete information about MLD-snooping of the specified vlan

Example

The following example shows how to display the information about MLD snooping of the specified vlan

switch#**show ipv6 mld-snooping vlan 1**

```
Vlan 1:
----------
    Running
    Ports:          g0/1      g0/2      g0/3      g0/4      g0/5      g0/6      g0/8      g0/9      g0/10     g0/11
g0/12     g0/13     g0/14
            g0/16     g0/17     g0/18     g0/19     g0/20     g0/21     g0/22     g0/23     g0/24
     Routers:
     No querier, MLD snooping doesn't work on this vlan
```

37.11 show ipv6 mld-snooping timer

Syntax

show ipv6 mld-snooping timer

Parameter

None

Default

None

Usage Guidelines

This command is used to display the information about the MLD-snooping clock

Example

The following example shows how to display the information about the MLD-snooping clock

switch#show ipv6 mld-snooping timer

vlan 1 Querier on port 0 : 251
vlan 2 Querier on port 0 : 251
vlan 2 multicast address 3333.0000.0005 response time : 13

switch#
Querier on port 0: 251: This shows the switch router aging timer expires.
vlan 2 multicast address 3333.0000.0005 response time: This shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled

37.12 show ipv6 mld-snooping groups

Syntax

show ipv6 mld-snooping groups

Parameter

None

Default

None

Usage Guidelines

This command is used to display the information about the multicast group of MLD-snooping

Example

The following example shows how to display the information about the multicast group of MLD-snooping

switch# show ipv6 mld-snooping groups

```
Vlan Group                Type Port(s)
---- ---------------- ---- -------------------------------------
     2 FF02::1:FF00:2    MLD    G0/2
     2 FF02::1:FF61:9901 MLD    G0/2
     1 FF02::1:FF13:394 MLD    G0/1
     1 FF02::1:FF00:2    MLD    G0/1
     1 FF02::1:FF00:12 MLD    G0/1
     1 FF02::1:FF13:647D MLD    G0/2
switch#
```

37.13 show ipv6 mld-snooping statistics

Syntax

show ipv6 mld-snooping statistics

Parameter

None

Default

None

Usage Guidelines

This command is used to display the information about MLD-snooping statistics

Example

The following example shows how to display the information about MLD-snooping statistics

switch#show ipv6 mld-snooping statistics

v1_packets:0 Quantity of MLD v1 packets

v2_packets:6 Quantity of MLD v2 packets

general_query_packets:5 Quantity of general query packets

special_query_packets:0 Quantity of special query packets

listener_packets:6 Quantity of Report packets

done_packets:0 Quantity of Leave packets

send_query_packets:0 Send the packets quantity of Query

err_packets:0 Quantity of error packets

37.14 show ipv6 mld-snooping mac

Syntax

show ipv6 mld-snooping mac

Parameter

None

Default

None

Usage Guidelines

This command is used to display the multicast MAC of MLD snooping

Example

The following example shows how to display the multicast MAC of MLD snooping

```
switch#show ipv6 mld-snooping mac
Vlan Mac                          Ref Flags
---- ---------------- ---- ------
   1 3333:0000:0001       1     2
   2 3333:ff61:9901       1     0
          FF02::1:FF61:9901
   1 3333:0000:0002       1     2
   1 3333:ff00:0002       1     0
          FF02::1:FF00:2
   1 3333:ff00:0012       1     0
          FF02::1:FF00:12
   1 3333:ff13:647d       1     0
          FF02::1:FF13:647D
   2 3333:ff00:0002       1     0
          FF02::1:FF00:2
   1 3333:ff13:0394       1     0
          FF02::1:FF13:394
   1 3333:ff00:0001       1     2
   1 3333:ff8e:7000       1     2
switch#
```

Ref means the quantity of referred IPv6 addresses of MAC.

Flags means the debug output information, and 2 means the information need be sent to CPU

Chapter 38 Basic Multicast Commands

38.1 debug ip mpacket

Syntax

If you want to track the process for the multicast packet, you can use **debug ip mpacket** command, and use the no form of the command to close debug information

debug ip mpacket [**access-list**][*group-address*][**detail**]

no debug ip mpacket

Parameter

parameter	Description
access-list	Range for tracked multicast packets
group-address	The tracked multicast packet group address
detail	Details for multicast packet processing

Default value

Disable debug information output

Command mode

EXEC

Usage guidelines

You can use this command to track the main process for multicast packet

Example

The following example shows some situations for multicast packet processing

You have received the (100.168.20.151, 224.1.1.1) packet on e0/1 port, and the packet length is 112 bytes

You have sent the (192.168.20.99, 224.0.0.5) packet on e0/1 port, and the packet length is 64 bytes

switch#debug ip mpacket

M INPUT : IP Vlan1 (100.168.20.151, 224.1.1.1) , len=112

M OUTPUT : IP Vlan1 (192.168.20.99, 224.0.0.5) , len=64

Related command

None

38.2 debug ip mroute-cache

Syntax

Use **debug ip mroute-cache** command to enable multicast routing cache tracking function, then you can see the change from the multicast routing cache. In addition, you can use the no format of the command to disable the tracking

debug ip mroute-cache [*group-address*]

no debug ip mroute-cache

Parameter

parameter	Description
group-address	The tracked multicast routing cache group address

Default value

Disable all tracking functions

Command mode

EXEC

Usage Guidelines

You can use this command to see the change of the adding/deleting of multicast routing cache

Example

The following example shows you some changes on the multicast routing cache, and the creating and timeout of (192.168.20.97, 230.0.0.1) cache

switch#debug ip mroute-cache

MRC: create (192.168.20.97, 230.0.0.1) mroute-cache

MRC: expired (192.168.20.97, 230.0.0.1) mroute-cache

Related command

None

38.3 debug ip multicast

Syntax

You can use **debug ip multicast** command to enable multicast event tracking function, and then see the interaction between the multicast protocol and mrouting. you can use the **no** format of the command to

disable the function

debug ip multicast [**alert** | **border-router**]

no debug ip multicast [**alert** | **border-router**]

Parameter

parameter	Description
alert	Track the alert interaction among multicast routing components
border-router	Track related events of multicast border router MBR

Default value

Disable all tracking functions

Command mode

EXEC

Usage guidelines

Defining some standard events between multicast routing protocol and mrouting indicates **alert**, such as creation alert and deletion alert which related (S, G). You can use **debug ip multicast alert** to see these alerts

BDCOM's multicast routing protocol supports MBR, and each multicast routing protocol is a "component". You can use **debug ip multicast border-router** command to see the component's running information

Example

In the following example, the alert router is turned on for output:

switch#debug ip multicast alert

MBR: [(S, G) deletion alert], originated by PIM-DM, sent to all components

MBR: [(S, G) creation alert], originated by NONE, sent to all components

MBR: src = 192.168.20.110, grp = 239.0.0.100

MBR: sent to owner PIM-DM first

MBR: [(S, G) join alert], originated by NONE, sent to PIM-DM

MBR: src = 192.168.20.110, grp = 239.0.0.100

MBR: [(S, G) firstuse alert], originated by NONE, sent to PIM-DM

MBR: src = 192.168.20.110, grp = 239.0.0.100

MBR: [(S, G) deletion alert], originated by PIM-DM, sent to all components

MBR: src = 192.168.20.110, grp = 239.0.0.100

38.4 ip multicast-statistic

Syntax

To enable IP multicast packet statistics, run the following command. To return to the default setting, use the no form of this command

ip multicast-statistic

no ip multicast-statistic

Parameter

None

Default value

Disabled

Command mode

Global configuration mode

Usage guidelines

The multicast statistics provides with evidence of switching rpt of pim-sm to spt. When configured switching threshold, the command needs to be enabled. Once the command is disabled, the switch will not make statistics of the multicast

Example

The following example shows how to configure the statistics multicast packet of the switch:

switch_config#ip multicast-statistic

Related Command

None

38.5 ip multicast-routing

Syntax

Use this command **ip multicast-routing** to enable IP multicast packet transferring function, and **no ip multicast-routing** to disable the function

ip multicast-routing

no ip multicast-routing

Parameter

None

Default value

The default is not to transfer multicast packets

Command mode

Global configuration mode

Usage Guidelines

If you disable this function, the router will no longer transfer multicast packets. Meanwhile, the multicast routing list and the multicast cache will be empty

Example

The following example will configure the router to transfer multicast packets:

switch_config#ip multicast-routing

Related command

show ip mroute mfc

38.6 ip multicast route-limit

Syntax

Use this command **ip multicast route-limit** to configure the maximum number of multicast routing item, and **no ip multicast route-limit** to un-limit the number

ip multicast route-limit *size*

no ip multicast route-limit *size*

Parameter

parameter	Description
size	Maximum number of multicast routing item, the range is from 1 to 5120

Default value

The default multicast routing item number is 5120 by default

Command mode

Global configuration mode

Usage guidelines

If you have configured this function, the multicast routing item number will be limited

Example

The following example will configure the maximum number of multicast routing list to 2000:

switch_config#ip multicast route-limit 2000

Related command

show ip mroute mfc

38.7 ip multicast boundary

Syntax

Use this command **ip multicast boundary** to manage the range for the port allowed processing multicast packets; it is valid for input/output packets on the port. Use **no ip multicast boundary** to cancel this command

ip multicast boundary *access-list*

no ip multicast boundary

Parameter

parameter	Description
access-list	the access-list name used to specify the range for processing multicast packets

Default

Process all multicast packets

Command mode

Interface configuration mode

Usage Guidelines

If the function is configured, the range for the port allowed processing multicast packets will be limited

Example

The following example will configure the range for the port vlan1 allowed processing multicast packets to the range limited by the access-list testacl:

switch_config_v1#ip multicast boundary testacl

Related command

None

38.8 ip multicast helper-map

Syntax

Use this command **ip multicast boundary helper-map** to configure the connection of two broadcast networks with the multicast routing on the multicast network, and **no ip multicast boundary helper-map** to cancel this command

ip multicast boundary helper-map {*group-address* | **broadcast**} {*broadcast-address* |*multicast-address*} *access-list*

no ip multicast boundary helper-map {*group-address* | **broadcast**} {*broadcast-address* | *multicast-address*}

Parameter

parameter	Description
group-address	The multicast packet group address which needed to be converted to the broadcast packet. it is used with the broadcast-address keyword
broadcast	It can convert the broadcast packet to the multicast packet. it is used with the multicast-address keyword
broadcast-address	The target address of broadcast packet which is sent after converting. it is used with the group-address keyword
multicast-address	The target address of multicast packet which is sent after converting. It is used with the broadcast keyword
access-list	IP extended access-list name. You can use it to specify the port number for packet converting

Default value

Not perform the conversion between any multicast packets and broadcast packets

Command mode

Interface configuration mode

Usage Guidelines

If two broadcast networks are connected with a multicast network, you can convert the broadcast flow to multicast flow on the first hop router connected with the source broadcast network, and then convert the multicast flow to broadcast flow on the last hop router connected with the target broadcast network. Thus, you can utilize the multicast network's multicast characteristic between the two broadcast networks which are required to be connected with each other. Furthermore, it can prevent the packets between two broadcast networks from being sent repeatedly, and utilize the "quick forward" characteristic on the multicast network

Before using **ip multicast helper-map**, you should have configured this command **ip directed-broadcast** on the port

Example

Configuration on the router is as follow:

If you configure command **ip directed-broadcast** on interface vlan1 of the first hop router, it will be allowed to process the link broadcast packets

If you have configured "ip multicast helper-map broadcast 230.0.0.1 testacl1", you can convert the udp broadcast packet, whose port number is 4000 ("ip forward-protocol" command specified) and the source address is 192.168.20.97/24 (testacl1 specified) , to multicast packet whose target address is 230.0.0.1 ("ip multicast helper-map" command specified)

if you configure command"ip directed-broadcast" on port vlan2 of the last hop router, it will be allowed to process the link broadcast packets

If you have configured "ip multicast helper-map broadcast 230.0.0.1 172.10.255.255 testacl2", you can convert the multicast packet, whose port number is 4000("ip forward-protocol" command specified), the source address is 192.168.20.97/24 (testacl2 specified) and target address is 230.0.0.1 , to broadcast packet whose target address is 170.10.255.255 ("ip multicast helper-map" command specified).

On the first hop router which is connected with the source broadcast network:

interface vlan1

ip directed-broadcast

ip multicast helper-map broadcast 230.0.0.1 testacl

ip pim-dm

!

ip access-list extended testacl

permit udp 192.168.20.97 255.255.255.0 any

!

ip forward-protocol udp 4000

On the last hop router which is connected with the target broadcast network:

interface vlan2
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim-dm
!
ip access-list extended testacl2
permit udp 192.168.20.97 255.255.255.0 any
!
ip forward-protocol udp 4000

Related command

ip forward-protocol

ip directed-broadcast

38.9 ip multicast ttl-threshold

Syntax

Use this command "ip multicast ttl-threshold" to configure the maximum threshold value of multicast packet ttl on the port, and "no ip multicast ttl-threshold" to restore default

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

Parameter

parameter	Description
ttl-value	The multicast packet ttl threshold value on the port. The range is from 0 to 255

Default

The default ttl threshold value on the port is 1

Command mode

Interface configuration mode

Usage Guidelines

The ttl value of receiving/sending packet should be largerer than the specified threshold value on the port, you can use this command to configure a router to border router

Example

The ttl threshold value configured on port vlan1 is 200, it means only the multicast packet with ttl value more than 200 is allowed to be received/sent on the port

interface vlan1
ip multicast ttl-threshold 200

Related command

None

38.10 show ip mroute-cache

Syntax

use this command "show ip mroute-cache" to display the information on the multicast routing cache

show ip mroute-cache [*group-address* [source-address]]

Parameter

parameter	Description
group-address	The displayed multicast routing cache group address
source-address	The displayed multicast routing cache source address

Default

none

Command mode

EXEC

Usage Guidelines

MRC (Multicast Route Cache) is a global multicast routing cache, and every MRC item contains the (S, G)/ (*, G) information, upstream/downstream interface information received from the multicast routing

Example

The following example will display multicast routing list information:

switch#show ip mroute-cache

IP Multicast Route Cache

(192.168.20.97, 230.0.0.1)|(192.168.20.97, 230.0.0.1)

Incoming interface: Vlan2, Last used : 00: 00: 34

Outgoing interface list:

Loopback0

(192.168.20.97, 230.0.0.2)|(192.168.20.97, 230.0.0.2)

Incoming interface: Vlan2, Last used : 00: 00: 12

Outgoing interface list:

Loopback1

38.11 show ip mroute mfc

Syntax

You can use this command “show ip mroute mfc” to display the multicast forwarding list information. You can add the vrf subcommand to display the multicast routing table under a certain vrf. If you do not add the subcommand, the global multicast routing table will be displayed

show ip mroute [vrf vrf_name] mfc

Parameter

Vrf vrf_name

Default

none

Command mode

EXEC

Usage guidelines

MFC (Multicast Forwarding Cache) is a global multicast forwarding list, and the multicast packet is forwarded by it. Every MFC item has (S, G)/ (*, G) information and upstream/downstream interface information

Example

The following example will display multicast routing list information:

switch#show ip mroute mfc

IP Multicast Forwarding Cache

(192.168.20.110/32, 239.0.0.100/32)

Incoming interface: Vlan2, RPF nbr 0.0.0.0, owned by PIM-DM

Outgoing interface list:

Loopback0, owned by PIM-DM

(192.168.20.110/32, 239.0.0.101/32)

Incoming interface: Vlan2, RPF nbr 0.0.0.0, owned by PIM-DM

Outgoing interface list:

Loopback0, owned by PIM-DM

(192.168.20.138/32, 239.1.1.1/32)

Incoming interface: Vlan2, RPF nbr 0.0.0.0, owned by PIM-DM

Outgoing interface list:

Loopback0, owned by PIM-DM

Related command

None

Chapter 39 IGMP Configuration Commands

39.1 clear ip igmp group

Syntax

If you want to clear the multicast group member information saved in multicast router that supports IGMP, you can use the command "**clear ip igmp group**"

clear ip igmp group [*type number*] [*group-address* | <cr>]

Parameter

parameter	Description
type-number	port type and port number
group-address	Multicast group's group address to clear information

Default value

None

Command mode

EXEC

Usage guidelines

Using this command, you can clear the multicast group member information saved in router when the saved multicast group information has a problem

Example

The following example shows you how to clear the information of multicast group 233.33.1.1 on port vlan 1.

clear ip igmp group vlan 1 233.33.1.1

Related command

None

39.2 debug ip igmp

Syntax

If you want to track the process for igmp-router end protocol, you can use this command "**debug ip igmp**", and use the"**no**" form of the command to disable debug information

debug ip igmp

no debug ip igmp

Parameter

None

Default value

Disable debug information output

Command mode

EXEC

Usage guidelines

You can use this command to track the main process for igmp-router end protocol to find the reason for protocol processing failure

Example

igmp-router function module's debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information

Related command

None

39.3 debug ip igmp-host

Syntax

If you want to track the process for igmp-host end protocol, you can use this command "**debug ip igmp-host**", and use the"**no**" form of the command to disable debug information

debug ip igmp-host [*group-address*]

no debug ip igmp-host [*group-address*]

Parameter

None

Default value

Disable debug information output

Command mode

EXEC

Usage guidelines

You can use this command to track the main process for igmp-host end protocol to find the reason for protocol processing failure

Example

Igmp-host function module's debug information usually use the natural language to make description. Due to its simplicity, we will not list all of the debug information

Related command

None

39.4 ip igmp helper-address

Syntax

If you want a port to transit IGMP packet, you can use this command to configure the port. One port can configure the command only once time, so the next configured command will overwrite the original command

ip igmp helper-address *destination-address*

no ip igmp helper-address *destination-address*

Parameter

parameter	Description
destination-address	the destination address of transitting IGMP packet

Default value

The port will not transit IGMP packet

Command mode

Interface configuration mode

Usage guidelines

Use this command "ip igmp helper-address" to transit all received igmp packets

Example

ip igmp helper-address 192.168.20.10

Related command

None

39.5 ip igmp join-group

Syntax

If you want to add a multicast group on the port, you can use this command to perform it

ip igmp join-group *group-address* [{**include|exclude**} *source-address*]

no ip igmp join-group *group-address* [{**include|exclude**} *source-address*]

Parameter

parameter	Description
group-address	the multicast group required to be added to the port
include	The mode of SSM needed to add a multicast group is "include"
exclude	The mode of SSM needed to add a multicast group is "exclude"
source-address	source filter address whose port is added to multicast group

Default value

No multicast group will be added to the port

Command mode

Interface configuration mode

Usage guidelines

Use this command "ip igmp join-group" to dynamically add a multicast group to the port

Example

ip igmp join-group 230.0.0.1
ip igmp join-group 230.0.0.1 exclude 192.168.20.10

Related command

None

39.6 ip igmp immediate-leave group-list

Syntax

If you want the router port running IGMP version 2 to run the multicast group function "Exit Now", you can use this command "**ip igmp immediate-leave group-list**" to perform configuring. In addition, you can use the "no" format of the command to forbid the IGMP host to "leave now"

ip igmp immediate-leave group-list *list-name*

no ip igmp immediate-leave

Parameter

parameter	Description
list-name	Pre-configured ip standard access-list name

Default value

The IGMP host is not allowed to run "Leave Now" function

Command mode

global configuration mode/Interface configuration mode

Usage guidelines

This command is available only for the port of running IGMP version 2. It can be used when the network connecting with the port has only one IGMP host. Through configuring this command, the host can immediately leave from a multicast group without the process for packet exchanging and delaying from the router. Besides, you can configure this command in global configuration mode and Interface configuration mode, but this command configured in global configuration mode will be prior to the command configured in Interface configuration mode. If you have configured the command in global configuration mode, the next command configured in Interface configuration mode will be ignored. On the other hand, the command configured in global configurationmode will overwrite the original command configured in interface configurationmode

Example

Prefer to "Configure multicast routing"

Related command

ip access-list

39.7 ip igmp last-member-query-interval

Syntax

To change the query interval of last group member on the current port, use this command "**ip igmp last-member-query-interval**". You can use the "no" format of the command to restore default settings

ip igmp last-member-query-interval *time*

no ip igmp last-member-query-interval

Parameter

parameter	Description
time	the value of last member query interval configured on the port. Its unit is millisecond. The range is from 100 to 65535

Default value

The default of the last group member query interval on the port is 1000ms

Command mode

Interface configuration mode

Usage guidelines

You can use this command "ip igmp last-member-query-interval" to modify the last group member query interval on the port

Example

The following example will modify the last member query interval on the port to 2 seconds

```
interface vlan 1
ip igmp last-member-query-interval 2000
```

Related command

None

39.8 ip igmp querier-timeout

Syntax

You can use this command "**ip igmp querier-timeout**" to modify other routers for IGMP querier timeout. Use the "no" format of this command to restore default

ip igmp querier-timeout *time*

no ip igmp querier-timeout

Parameter

parameter	Description
time	other querier timeout. Its unit is second. The range is from 60 to 300

Default value

125 seconds

Command mode

Interface configuration mode

Usage guidelines

You can use this command "ip igmp querier-timeout" to modify other routers for querier timeout. This command is available only for the port which running IGMP version 2

Example

The following example shows that the querier-timeout specified on interface vlan 1 is 100 seconds

interface vlan 1

ip igmp querier-timeout 100

Related command

None

39.9 ip igmp query-interval

Syntax

To set the interval for IGMP General Query packet sending on the port, you can use this command "**ip igmp query-interval**". Use the "no" format of this command to restore default

ip igmp query-interval *time*

no ip igmp query-interval

Parameter

parameter	Description
time	interval of sending general query packet. Its unit is second. The range is form 2 to 65535

Default value

60 seconds

Command mode

Interface configuration mode

Usage guidelines

You can use this command "**ip igmp query-interval**" to set the interval for general query packet sending on the port

Example

The following example shows that the interval of sending general query packet on port is specified vlan 1 to 50 seconds

interface vlan 1

ip igmp query-interval 50

Related command

None

39.10 ip igmp query-max-response-time

Syntax

To specify the maximum interval for IGMP host to respond General Query packet, you can use this command "**ip igmp query-max-resposne-time**". Use the "no" format of this command to restore default

ip igmp query-max-response-time *time*

no ip igmp query-max-response-time

Parameter

parameter	Description
time	value of the maximum response time configured on the port. The range is from 1 to 25

Default

10 seconds

Command mode

Interface configuration mode

Usage guidelines

You can use this command "**ip igmp query-max-response-time**" to specify the maximum interval for IGMP host to respond General Query packet. This command is available only for the port which running IGMP version 2 and 3

Example

The following example will set the IGMP maximum response time on port vlan 1 as 15 seconds.

interface vlan 1

ip igmp query-max-response-time 15

Related command

None

39.11 ip igmp static-group

Syntax

If you want to configure a static multicast group on the port, you can use this command "**ip igmp static-group**" to perform it. Use the "no" format of this command to restore default

ip igmp static-group { ***** | *group-address* } {**include** *source-address* | <cr> }

no ip igmp static-group { ***** | *group-address* } {**include** *source-address* | <cr> }

Parameter

parameter	Description
*	all multicast groups
group-address	specified multicast group address
source-address	specified host source address

Default value

In default, no multicast group is static configured on the port

Command mode

Interface configuration mode

Usage guidelines

Configure the static IGMP multicast group information on the current port

Notes:

For the same group-address, you can configure several "include source-address" commands for the corresponding static multicast group to have several source-addresses existing. However, for the same group-address, you can't configure both commands with/without "include source-address"

Example

Refer to "Configure multicast routing"

Related command

None

39.12 ip igmp version

Syntax

To set the IGMP version number running on the port, you can use this command "**ip igmp version**". Use the "no" format of the command to restore default

ip igmp version *version-number*

no ip igmp version

Parameter

parameter	Description
version-number	The value 1, 2 or 3 indicates separately the IGMP version number 1, 2 or 3

Default value

If you don't configure this command, the default version number for IGMP-Router end protocol running on the port is 3

Command mode

Interface configuration mode

Usage guidelines

Use this command "**ip igmp version**"can set the IGMP version number running on the port

Example

The following example will specify the IGMP version number running on port vlan 1 as 2.

interface vlan 1

ip igmp version 2

Related command

None

39.13 show ip igmp groups

Syntax

You can use the following command to see the multicast group member information that is saved on the current router

show ip igmp groups {**interface** | *group-address* | **detail**}

Parameter

parameter	Description
interface	The port where you want to see the multicast group information. If you don't add this

	parameter, all multicast groups information on the port will be displayed
group-address	The multicast group address to see. If you don't add this parameter, all multicast groups information on the router will be displayed
detail	T he router whether you want to see the multicast group information

Default value

None

Command mode

EXEC/global configuration mode/Interface configuration mode

Usage guidelines

You can use this command to see the multicast group member information that is saved on the router

Example

show ip igmp groups detail

Running this command will display the following message:

.....

Interface: VLAN1

Group address: 233.33.1.3

Uptime: 00: 03: 46

Group status: Static

Group filter mode: INCLUDE

Last reporter: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

Source address: Uptime Timer Fwd Flags

192.168.20.5 00: 03: 46 stopped Yes S

Interface: VLAN1

Group address: 233.33.1.1

Uptime: 00: 03: 46

Group status: Static

Group filter mode: INCLUDE

Last reporter: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

Source address:	Uptime	Timer	Fwd	Flags
192.168.20.5	00: 03: 46	stopped	Yes	S
192.168.20.3	00: 03: 46	stopped	Yes	S
192.168.20.1	00: 03: 46	stopped	Yes	S

.....

show ip igmp groups 233.33.1.1 detail

Running this command will display the following message:

Interface: VLAN1

Group address: 233.33.1.1

Uptime: 00: 02: 42

Group status: Static

Group filter mode: INCLUDE

Last reporter: 0.0.0.0

Group source-list: (Flags: S-Static, R-Remote)

Source address:	Uptime	Timer	Fwd	Flags
192.168.20.5	00: 02: 42	stopped	Yes	S
192.168.20.3	00: 02: 42	stopped	Yes	S
192.168.20.1	00: 02: 42	stopped	Yes	S

show ip igmp groups

Running this command will display the following message:

Interface	Group address	Uptime	Expires	Last Reporter	Flags
VLAN1	239.255.255.250	00: 01: 08	00: 02: 05	192.168.20.141	R
VLAN1	224.2.127.254	00: 01: 09	00: 02: 00	32.1.1.67	R
VLAN1	224.1.1.1	00: 01: 24	stopped	0.0.0.0	S
VLAN1	233.33.1.5	00: 01: 24	stopped	0.0.0.0	S
VLAN1	233.33.1.3	00: 01: 24	stopped	0.0.0.0	S
VLAN1	233.33.1.1	00: 01: 24	stopped	0.0.0.0	S

Interface	Group address	Uptime	Expires	Last Reporter	Flags
Loopback10	239.255.255.250	00: 01: 08	00: 02: 05	192.168.20.141	R
Loopback10	224.2.127.254	00: 01: 09	00: 02: 00	32.1.1.67	R

Related command

None

39.14 show ip igmp interface

Syntax

You can use this command to see information on the current router's port where IGMP is activated

show ip igmp interface { **interface** | <cr> }

Parameter

parameter	Description
interface	The specified port to display information. If you don't add this parameter, all information on ports where IGMP is activated will be displayed

Default value

None

Command mode

EXEC/global configuration mode/Interface configuration mode

Usage guidelines

You can use this command to display information on the port where IGMP is activated

Example

show ip igmp int vlan 1

Running this command will display the following information:

VLAN1 is up, line protocol is up

Internet address is 192.168.20.167

Current IGMP switch version is 3

switch plays role of querier on the interface now

IGMP is enable on the interface

IGMP query-interval is 60 seconds

IGMP max query response time is 10 seconds

IGMP Last member query response time is 1000 milliseconds

IGMP querier timeout is 125 seconds

Multicast routing is enabled on the interface

Related command

None

39.15 show ip igmp-host

Syntax

You can use this command to see IGMP host information on the port ofcurrent router

show ip igmp-host { **interface** } [**detail**]

Parameter

parameter	Description
interface	The specified port to display information
detail	Display igmp host detailed information

Default value

none

Command mode

EXEC/global configuration mode/Interface configuration mode

Usage guidelines

You can use this command to display basic IGMP host information on the port

Example

show ip igmp-host interface vlan 1

Running this command will display the following information:

IGMP host Mode is IGMP_V3_switch

IGMP host Query Interval is 23 second

IGMP host Query Response Interval is 125

IGMP host Query Robustness Variable is 2

IGMP host Last Query Interval is 0

IGMP interface timer is 0

IGMP host group joined(number of users):

230.0.0.1(1)

Related command

None

Chapter 40 PIM-DM Configuration Commands

40.1 clear ip mroute pim-dm

Syntax

Use the following command in EXEC to clear the (S, G) routing list items submitted by PIM-DM to mrouting:

clear ip mroute pim-dm {***** | **group** [**source**]}

Parameter

parameter	Description
*****	Delete all multicast routing list items submitted by pim-dm
group	Delete all list items submitted by pim-dm and satisfied in the specified group
source	(optional) Delete all list items submitted by pim-dm and satisfied in the specified group's *source*

Default value

None

Command mode

EXEC

Usage guidelines

The command will delete all or part of table lists of local multicast router table, and it is possible to affect the normal multicast packet forwarding. This command can only delete the (S, G) items, whose upstream port is created by PIM-DM multicast routing protocol, and inform mrouting, then mrouting will determine if it should re-establish the corresponding (S, G)

Example

Example1:

Switch#clear ip mroute pim-dm *

All (S, G) items, whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared

Example2:

Switch #clear ip mroute pim-dm 239.1.1.1

All (S, G) items with the group address 239.1.1.1, whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared

Example3:

Switch #clear ip mroute pim-dm 239.1.1.1 192.168.20.131

All (S, G) items with the address (192.168.20.138, 239.1.1.1), whose middlestream/upstream port is created by PIM-DM, on local MRT will be cleared

40.1.1 debug ip pim-dm

Syntax

Use this command to track input/output PIM packets and caused events. Set this command to "no" to stop tracking

debug ip pim-dm [**group** | **alert | assert | graft | hello | jp | neighbor | packet | sg | state-refresh | timer**]

Parameter

parameter	Description
group	(optional) Track the specified group status
alert	(optional) Track the alert status received from mrouting
assert	(optional) Track the status of asset information
graft	(optional) Track grafting information
hello	(optional) Tracking neighbors' hello message sending and receiving
jp	(optional) Track join/prune messages
neighbor	(optional) Track changes in neighbors
packet	(optional) Tracking the sending and receiving of messages
sg	(optional) Track changes in sg entrie.
state-refresh	(optional) Track status refresh packet
timer	(optional) Track the triggering of various timers

Default value

None

Command mode

EXEC

Usage guidelines

Receive Alert from mrouting

Send alert to other components

Example

The following example shows debugging information of group and alert

Example 1, the output information is as follows:

Hello packet prompt sent to each port.

Hello packet prompt received from each port.

A new neighbor is found.

Delete neighbor.

Port sending status refresh packet.

Port receiving status refresh packet.

Port is sending Assert packet.

Port is receiving Assert packet.

Port is sending prune packet.

Port is receiving prune packet.

Port is sending graft ack packet.

Port is receiving graft ack packet.

Port is sending graft packet.

Port is receiving graft packet.

Port is sending join/prune packet.

Port is receiving join/prune packet.

When a new (S, G) is created

When deleting (S, G)

switch#debug ip pim-dm

2003-3-26 11: 45: 17 received V2 hello packet on Vlan2 from 192.168.20.133(GenID = 3539)

2003-3-26 11: 45: 17 Vlan2 create new nbr 192.168.20.133

2003-3-26 11: 45: 25 send hello packet to 224.0.0.13 on Loopback1

2003-3-26 11: 50: 29 Vlan2 delete nbr 192.168.20.133

2003-3-26 11: 50: 51 received V2 hello packet on Vlan2 from 192.168.20.152

2003-3-26 11: 50: 51 send hello packet to 224.0.0.13 on Vlan2

2003-3-26 12: 04: 37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success

2003-3-26 12: 04: 37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful

2003-3-26 12: 04: 39 PIM-DM: ignored V2 packet on Vlan2 from 192.168.10.204 (validate source address failed)

2003-3-26 12: 04: 39 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream: 192.168.20.132 Adding in MRT success

2003-3-26 12: 04: 39 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

Example 2, output received alert message:

switch#debug ip pim-dm alert

2003-3-26 12: 09: 51 receive alert_rt_change alert from mroute

2003-3-26 12: 09: 54 receive alert_rt_change alert from mroute

2003-3-26 12: 11: 08 PIM-DM: send sg_deletion alert

2003-3-26 12: 11: 19 receive alert_sg_creation alert from mroute

2003-3-26 12: 11: 20 receive alert_sg_prune alert from mroute

2003-3-26 12: 11: 56 receive alert_group_report alert from mroute

2003-3-26 12: 11: 56 receive alert_sg_join alert from mroute

Example 3, track the specified group status:

switch#deb ip pim-dm 239.1.1.1

switch#2003-3-26 12: 35: 27 PIM-DM: clear (192.168.20.138, 239.1.1.1) forwd pkt count success

2003-3-26 12: 35: 37 PIM-DM: delete (192.168.20.138, 239.1.1.1) in MRT success

2003-3-26 12: 35: 37 PIM-DM: clear (192.168.20.138, 239.1.1.1) from MRT successful

2003-3-26 12: 35: 37 PIM-DM: (192.168.20.138, 239.1.1.1)'s upstream: 192.168.20.132 Adding in MRT success

2003-3-26 12: 35: 37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 1.1.1.1 create success

2003-3-26 12: 35: 37 PIM-DM: (192.168.20.138, 239.1.1.1)'s downstream: 192.167.20.132 create success

2003-3-26 12: 35: 42 PIM-DM: (192.168.20.138, 239.1.1.1) Adding in MRT

40.2 ip pim-dm

Syntax

This command is used to run PIM-DM on the port. Use no form of this command to disable PIM-DM on the port

ip pim-dm

no ip pim-dm

Parameter

None

Default

None

Command mode

Interface configuration mode

Usage guidelines

1.If the "ip multicast-routing" is not configured before configuring this command, it will display the following warning: WARNING: "ip multicast-routing" is not configured, IP Multicast packets will not be forwarded

2.Once this function is disabled, PIMDM will no longer run on the port, but it will not affect other PIM-DM configurations. After re-running PIM-DM on the port, all PIM-DM configurations are still valid

3.Enabling this function means it is available for forwarding multicast packet on the port. Certainly, you have to enable the global multicast packet forwarding function first

Example

Switch_config#ip multicast-routing

Switch_config#interface vlan 1

Switch_config_v1#ip pim-dm

Related command

ip multicast-routing

show ip pim-dm interface

40.3 ip pim-dm dr-priority

Syntax

Set a router as the priority to specified router (DR). You can set this command to "no" to restore default DR priority on the port

ip pim-dm dr-priority priority

no ip pim-dm dr-priority

Parameter

parameter	Description
priority	Port DR priority. The larger the value is, the higher the priority is. Its range is from 0 to 4294967294, and the default is 1

Default value

Default DR priority on PIM port is 1

Command mode

Interface configuration mode

Usage guidelines

1.If all PIM neighbors support DR Priority on the port, select the one with the highest priority as DR. If all have the same priority, just select the one with the highest port IP value as DR

2.If router didn't advertise its priority in Hello packet and there are several routers have the same situation, just select the router with the highest port IP value as DR

40.4 ip pim-dm hello-interval

Syntax

This command is used to configure the interval of regularly sent PIM-Hello packets on the port. You can set this command to "no" to restore default interval

ip pim-dm hello-interval *interval*

no ip pim-dm hello-interval

Parameter

parameter	Description
interval	The interval of regularly sent PIM-Hello packets. Its range is from 0 to 65535, and the default is 30 seconds

Default value

30 seconds

Command mode

Interface configuration mode

Usage guidelines

Regularly sending Hello packets can check if the neighbor exists. Generally, if Hello packets is not received after the 3.5 times hello-interval timeout configured by neighbor, the neighbor will be considered disappeared

For IGMP v1, you can select the specified router (DR) through PIM-DM Hello packet

Example

Switch_config#interface vlan 1

Switch_config_v1#ip pim-dm hello-interval 30

Related command

ip igmp query-interval

40.5 ip pim-dm state-refresh origination-interval

Syntax

The command allows the router to generate original PIM-DM state refresh packet and configure the state refresh interval. To cancel the generation for original PIM-DM state refresh packet, set this command to "no"

ip pim-dm state-refresh origination-interval [interval]

no ip pim-dm state-refresh origination-interval

Parameter

parameter	Description
interval	For the first port router connected with the source directly, it is the interval of regularly sending state refresh packet. For the following router, it is interval of allowed receiving and processing state refresh packet for the port This parameter is configured optionally, and its range is from 4 to 100 seconds. The default is 60 seconds

Default value

Refer to instructions for use

Command mode

Interface configuration mode

Usage guidelines

Configure this command on the first router's, neighboring directly on the multicast source, incoming port. By default, it will generate original state refresh packet. During configuring this command on the following router's port, you can use *interval* to limit the process for received state refresh packet interval. By default, all routers where is running PIM-DM can process and forward state refresh packet

Example

switch_config_v1#ip pim-dm state-refresh origination-interval 80

Related command

ip pim-dm state-refresh disable

40.6 ip pim-dm neighor-filter

Syntax

This command is used to prevent some routers from participating PIM-DM operation. Set this command to "no" to cancel the limit

ip pim-dm neighbor-filter *access-list-name*

no ip pim-dm neighbor-filter *access-list-name*

Parameter

parameter	Description
access-list-name	Standard access-list, whose definition is to deny PIM packets from the specified source

Default

No filter function

Command mode

Interface configuration mode

Usage guidelines

You can use multiple filter lists. The router denied by anyone of the lists can't be a neighbor of local PIM-DM

Example

switch_config_v1#ip pim-dm neighbor-filter nbr_filter

switch_config#ip access-list standard nbr_filter

switch_config_std#deny 192.167.20.132 255.255.255.255

switch_config_std#permit 192.168.20.0 255.255.255.0

Related command

access-list (IP standard)

40.6.1 show ip pim-dm neighbor

Syntax

To display the PIM-DM neighbor and the selected DR, run the following command:

show ip pim-dm neighbor [**interface-type** *interface-number*]

Parameter

Parameter	Description
interface-type *interface-number*	Type and ID of the interface, such as Ethernet1/1 and serial 11/0

Default value

None

Command mode

All modes except the user mode

Usage guidelines

This command is used to check on which LAN routers PIM-DM or PIM-SM is configured

Example

Example 1:

Switch#show ip pim-dm neighbor

PIM-DM Neighbor Table

Neighbor Address	Interface	Uptime/Expires	Ver	DR Prior/Mode
192.167.20.132	v1	03: 13: 34 / 00: 00: 00	v2	4/D (DR)
1.1.1.1	Loopback1	03: 52: 30 / 00: 00: 00	v2	1/D (DR)
192.168.20.132	v2	19: 35: 56 / 00: 00: 00	v2	1/D
192.168.20.152	v2	00: 00: 04 / 00: 01: 41	v2	1/D
192.168.20.204	v2	00: 00: 36 / 00: 01: 44	v2	20/D (DR)

Example 2:

switch# show ip pim-dm neighbor vlan 2

PIM-DM Neighbor Table

Neighbor	Interface	Uptime/Expires	Ver	DR Prior/Mode

Address

192.168.20.132	v2	19: 39: 22 / 00: 00: 00	v2	1/D	
192.168.20.152	v2	00: 00: 30 / 00: 01: 15	v2	1/D	
192.168.20.204	v2	00: 00: 04 / 00: 02: 16	v2	20/D	(DR)

Related command

ip pim-dm

ip pim-dm dr-priority

ip pim-dm hello-interval

ip pim version

ip pim-dm neighor-filter

show ip pim-dm interface

40.6.2 show ip pim-dm interface

Syntax

To display the state of the PIM-DM interface, run the following command:

show ip pim-dm interface [**interface-type** *interface-number*]

Parameter

Parameter	Description
interface-type *interface-number*	(optional)Type and ID of the interface, such as Ethernet1/1 and serial 11/0

Default value

None

Command mode

All modes except the user mode

Usage guidelines

Only the state of the PIM-DM interface can be displayed after this command is run. If the PIM-DM interface is not designated, the information about all PIM-DM interfaces' state will be displayed

Example

Example 1:

Switch#show ip pim-dm interface

address	Interface	Ver/ Mode	Nbr Count	Hello intvl	DR Prior	DR
192.167.20.132	v1	v2/D	0	30	4	192.167.20.132
1.1.1.1	Loopback1	v2/D	0	30	1	1.1.1.1
192.168.20.132	v2	v2/D	2	30	1	192.168.20.204

Example 2:

Switch#show ip pim-dm interface vlan 2

address	Interface	Ver/ Mode	Nbr Count	Hello intvl	DR Prior	DR
192.168.20.132	v2	v2/D	2	30	1	192.168.20.204

Related command

ip pim-dm

ip pim-dm dr-priority

ip pim-dm hello-interval

ip pim version

ip pim-dm neighor-filter

show ip pim-dm neighbor

40.6.3 show ip rpf pim-dm

Syntax

To display how the multicast route conducts the Reverse Path Forwarding (RPF), run the following command:

show ip rpf pim-dm *source-address*

Parameter

Parameter	Description
source-address	Displays the RFP information of the designated source address

Default value

None

Command mode

All modes except the user mode

Usage guidelines

The PIM-DM protocol can obtain the RPF information from multiple types of routing tables. This command tells you where the RPF information is obtained

Example

Switch#show ip rpf pim-dm 4.1.1.1

RPF information for (4.1.1.1)

RPF interface: vlan 2

RPF neighbor: 192.168.20.80

RPF route/mask: 192.168.20.0/24

RPF type: unicast

Metric preference: 120

Metric: 1

Related command

None

Chapter 41 PIM-SM Configuration Commands

41.1 ip pim-sm

Syntax

Use the **ip pim-sm** command to enable pim-sm on the port. Use **no ip pim-sm** command to disable this function on the port.

ip pim-sm

no ip pim-sm

Parameter

Parameter	English prompt
pim-sm	pim-sm -- Enable PIM protocol sparse mode

Default value

Disable PIM-SM

Command mode

INTERFACE CONFIGURATION MODe

Usage guidelines

Only when ip multicast-routing is configured in the global configuration mode, the pim-sm command can be used to enable pim-sm on the port

If pim-sm is configured for the port for the first time, the hello mechanism will be started, and IGMP will be enabled on the port. In addition, other port-dependent configurations in the global pim-sm configuration mode will be detected, and corresponding operations will be started (such as enabling the BSR election mechanism). For the first configuration, a hello message will be triggered on the port, and the trigger timer is a random value of 0 to 5 seconds

If **ip mulitcast-routing** is not configured in the global configuration mode, when the port is configured with **ip pim-sm** for the first time, there will be a prompt similar to the following:

WARNING: "ip multicast-routing" is not configured,

IP Multicast packets will not be forwarded

If other multicast protocols have been configured on the port, pim-sm cannot be configured

Example

The following example indicate the interface vlan8 will start PIM-SM multicast protocl

switch_config_v8#ip pim-sm

41.1.1 ip pim-sm admin-scope

Syntax

To configure the multicast administrator scope, run ip pim-sm admin-scope gaddr gmask. The designated multicast address ranges between 239.0.0.0 and 239.255.255.255. This command is configured only on the edge routers which interlace other SZs

ip pim-sm admin-scope *gaddr gmask*

no ip pim-sm admin-scope

Parameter

Parameter	English prompt	Remark
admin-scope	admin-scope – pim-sm administrator scope	Only the C-BSRs and the ZBRs need to be configured to know about the existence of the scope zones. Other routers, including the C-RPs, learn of their existence from Bootstrap messages.
gaddr	A.B.C.D -- private group address prefix	239.0.0.0 to 239.255.255.255
gmask	A.B.C.D -- private group mask	

Default value

The global domain is 224.0.0.0/4 by default

Command mode

Port configuration mode

Usage guidelines

This command is configured on the boundary of the PIM-SM administrator scope and used to check the BSM information which is received from the outside of the administrator scope. If the SZ scope of the received BSM information is smaller than or equal to the locally configured administrator scope, the received BSM information will be discarded. Otherwise, the received BSM information will enter the local administrator scope. When the BSM information is forwarded locally, the same principle is followed. At present, Huawei only supports the global domain and the private domain, but does not support the covering of the group address. RP in SZ1 will not notify the global SZ of the C-RP-ADV information. But the global BSM information can get in

Example

The following example shows how to configure the boundary scope on routerA to pim-sm sz1(239.1.1.1/24).

switchA_config_v8#ip pim-sm admin-scope 239.1.1.1 255.255.255.0

switchA_config_ps# c-bsr interface lo1

switchA_config_ps# c-bsr admin-scope 239.1.1.1 255.255.255.0

Related command

ip pim-sm bsr-border

c-bsr intf_type intf_name

41.1.2 ip pim-sm asrt-hold

Syntax

To configure the holdtime for the assert state on the port corresponding to PIM-SM, run the following command

ip pim-sm asrt-hold *intvl*

no ip pim-sm asrt-hold

Parameter

Parameter	English prompt	Remark
asrt-hold	asrt-hold -- assert status holdtime	
intvl	<7-65535> -- assert status hold timer value(uint: second, default: 180)	The default value is 180 seconds

Default value

180 seconds

Command mode

Port configuration mode

Usage guidelines

None

Example

The following example shows how to configure the timeout time in assert state on port vlan8 to 200 seconds.

switch_config_v8#ip pim-sm asrt-hold 200

41.1.3 ip pim-sm bsr-border

Syntax

To prevent BSM (bootstrap message) messages from receiving and sending on the specified port, use the command **ip pim bsr-border**. To cancel this restriction, you can use the no form of the command

ip pim-sm bsr-border

no ip pim-sm bsr-border

Parameter

Parameter	English prompt	Remark
bsr-border	bsr-border -- BSR border	

Default value

Disable

Command mode

Port configuration mode

Usage guidelines

This command can set interface to BSR boundary didn't send/receive BSM message. This command change difineition BSR boundary to make BSM message can not effect each other in different PIM-SM domain. Otherwise, PIM may elect RPs in other domains as the RPs of this domain, which will eventually cause functional disorder or lose the ability to isolate between domains

Example

The following example configures the interface to be the PIM domain border:

switch_config_v8# ip pim-sm bsr-border

Related command

None

41.1.4 ip pim-sm dr-pri

Syntax

Each pim port (LAN port or other type of port) will select a DR. Refer to the description of $2.3.3 for DR election rules. It should be emphasized that the DR priority value is given first priority to the port configuration, followed by the global configuration, and the default configuration takes the third place. After configuring the DR priority, you need to reset the hello timer and set the first timeout value as the value of triggering update PS_RAND_INTVAL(50)

ip pim-sm dr-pri *pri-value*

no ip pim-sm dr-pri

Parameter

Name	English prompt
dr-pri	dr-pri -- PIM-SM DR priority of the interface

Pri-value	<0-4294967295> -- DR priority, preference given to larger value

Default value

DR priority is 1 by default in global mode

Command mode

Interface configuration mode

Usage guidelines

The change of the global DR priority may affect the reselection of the DR of the port. The election of DR depends on whether the corresponding port itself and all neighbors under the port support DR priority; if it does, the DR with the higher DR priority value is selected as the DR. If the priority is the same, the DR with the higher IP address is used as the DR; DR priority is not fully supported, and the one with the larger IP address is directly used as the DR. If the port DR becomes non-DR or vice versa, it may be necessary to comprehensively consider the assert state machine and the corresponding actions of (s, g) and (*, g)

Example

The following example sets the DR priority value to 200 for the pim-sm interface vlan8:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm dr-pri 200

Related command

None

41.1.5 ip pim-sm hello-intvl

Syntax

Set the interval of the hello timer on the pim-sm port. The value range is 1 to 65535 in seconds. intvl×3.5 is the timeout period for local reachability

ip pim-sm hello-intvl *seconds*

no pim-sm hello-intvl

Parameter

Name	English prompt
hello-intvl	hello-intvl -- PIM-SM router hello advertisement interval
seconds	<1-65535> -- periodic pim hello message are sent(unit: s)

Default value

The interval of sending Hello messages is 30s

Command mode

Interface configuration mode

Usage guidelines

Port configuration takes precedence, configuration takes the second place, otherwise, the default value is select. After the Hello interval is configured, the default holdtime is set as 3.5 times of Hello interval correspondingly, which will be included in the hello message as an option

Example

The following example sets the hello interval value to 40 for interface vlan8:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm hello-intvl 40

Related command

None

41.1.6 ip pim-sm holdtime

Syntax

To configure the interval of the hello timer on the PIM-SM port, run the following first command. The value of the interval ranges between 4 and 65535. The unit is seconds

ip pim-sm holdtime *seconds*

no pim-sm holdtime

Parameter

Name	English prompt
Holdtime	Holdtime -- keep alive time to neighbor
seconds	<4-65535> -- keep alive time value(uint: s, default: 3.5x hlo_intvl)

Default value

105 seconds

Command mode

Interface configuration mode

Usage guidelines

This command is first run in port configuration mode and then in global configuration mode, or the default value is chosen. If the value of the holdtime is smaller than that of Hello interval, the configured value is then invalid. The value of the holdtime is 3.5 times of hello-intvl

Example

The following example sets the holdtime value to 100 for interface pim-sm configuration:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm holdtime 100

Related command

ip pim-sm hold-intvl

intvl-time hello hlo-intvl

41.1.7 ip pim-sm horizon-split

Syntax

To configure the horizon split strategy of the BSM packets on a port, run the following first command

ip pim-sm horizon-split

no ip pim-sm horizon-split

Parameter

Name	English prompt
horizon-split	horizon-split -- permit interface horizon split for BSM

Default value

The horizontal split is disabled by default

Command mode

Interface configuration mode

Usage guidelines

After this command takes effect, you can set the corresponding label bit of the PIM-SM port. The BSM packets that are received from a port will not be transmitted from the port

Example

The following example configures the bsm split horizon strategy to be enabled on the vlan8 port:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm horizon-split

Related command

bsm policy

41.1.8 ip pim-sm jp-hold

Syntax

To configure the holdtime for the join-prune state on the port corresponding to PIM-SM, run the following first command

ip pim-sm jp-hold *intvl*

no ip pim-sm jp-hold *[intvl]*

Parameter

Name	English prompt	Notes
jp-hold	jp-hold -- join-prune status holdtime	
intvl	<1-65535> -- jp state keep time value(uint: second, default: 210)	The default value is 210 seconds

Default value

210 seconds

Command mode

Port configuration mode

Usage guidelines

None

Example

The following example shows how to configure the timeout time in join state on port vlan8 to 200 seconds

switch_config_v8#ip pim-sm jp-hold 200

41.1.9 ip pim-sm jp-intvl

Syntax

To set the interval of transmitting the join or prune packets periodically, run the following first command. The interval, whose unit is second, ranges between 1 and 65535

ip pim-sm jp-intvl *seconds*

no **ip pim-sm jp-intvl**

Parameter

Name	English prompt	Notes
jp-intvl	jp-intvl -- Join/Prune message advertisement interval	
Seconds	<1-65535> -- regular Join/Prune message interval(unit: s, default: 60)	The default value is 60 seconds

Default value

60 seconds

Command mode

Port configuration mode

Usage guidelines

At each configuration the PIM-SM database must be entirely searched for the **(s, g)** pairs or the **(*, g)** pairs; if the configured port is an upstream one, the interval of the **jp** timer of the corresponding **(s, g)** or **(*, g)** pair should be reset. The interval in port configuration mode is prior to the **join/prune** interval in global mode. If the **Join** packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast item will be shifted to the **prune** state. The default holdtime is 3 minutes. If this value is changed randomly, CPU shock and service-forwarding shock may be caused.

Example

The following example changes the PIM join message interval to 90 seconds:

switch_config_v8# ip pim-sm jp-intvl 90

Related command

ip pim-sm jp-hold

41.1.10 ip pim-sm lan-delay

Syntax

To designate the prune delay time of the PIM-SM port, run the following first command. The local downstream port receives the prune message sent by the downstream switch, and the downstream port corresponding to

the multicast entry is switched to prune after the specified prune pending timer expires. The timeout interval of the PPT timer is negotiated according to delay-intvl

ip pim-sm lan-delay *delay-intvl*

no ip pim-sm lan-delay

Parameter

Name	English prompt	Notes
lan-delay	lan-delay- pim-sm prune delay	
delay-intvl	<0-32767> -- lan delay(uint: ms, default: 500)	The default value is 500 milliseconds

Default value

500ms

Command mode

Interface configuration mode

Usage guidelines

If the local port is the downstream port, the finally calculated prune delay time is based on all maximum values reported by downstream neighbors. In this case, the override timer of transmitting the **join** packets towards the upstream neighbors will be affected. If the **prune_delay** option is not supported by all downstream neighbors, the default value will be used as the overtime interval of the **prune pending** timer. If the interval of the **prune delay** timer is locally set, it will be reported to upstream neighbors through the HELLO packets.

Example

The following example sets the prune delay value to 200 ms for the pim-sm interface vlan8:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm lan-delay 200

Related command

ip pim-sm override

41.1.11 ip pim-sm nbma-mode

Syntax

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information.

ip pim-sm nbma-mode

no ip pim-sm nbma-mode

Parameter

Name	English prompt	Notes
nbma-mode	nbma-mode -- Enable NBMA mode	

Default value

Disable

Command mode

Interface configuration mode

Usage guidelines

Traditional NBMA networks (frame relay, ATM and SMDS) adopt the point-to-multipoint mode; when a sub-node need be pruned, it will report this information directly to the central node and other sub-nodes, however, can not receive this information. In this case, other sub-nodes cannot respond and the interface of the central node will be incorrectly pruned

If the following first command is configured on all NBMA interfaces, the central node will forward all information that is transmitted from the sub-nodes and the other sub-nodes can obtain the corresponding information

This command cannot be used in multicast LANs, such as Ethernet or FDDI. For NBMA networks such as frame relay, it is necessary to see which neighbors of the corresponding output port need to receive the multicast service data before unicasting the service data to the corresponding neighbors

This command is only used for networks that do not have multicast capabilities; and, this command can be configured only when pim-sm is configured on the port

Multicast service data is only sent to downstream neighbors that clearly need the multicast stream (using the multicast group as the destination address and sent in unicast mode), and these neighbors explicitly send join messages to the upstream port. This command can be configured only when pim-sm is configured on the port

Example

The following example configures an interface to be in NBMA mode:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm nbma-mode

Related command

None

41.1.12 ip pim-sm nbr-filter

Syntax

To stop a device from being added to PIM (for example, to configure stub multicast routing), run the following first command; to cancel this function, run the following second command

ip pim-sm nbr-filter *acl-name*

no ip pim-sm nbr-filter *[acl-name]*

Parameter

Name	English prompt	Notes
br-filter	nbr-filter -- PIM-SM neighbor filter	
acl-name	WORD -- Standard ACL name	

Default value

Disable

Command mode

Interface configuration mode

Usage guidelines

If this command is configured, the neighbors need be filtered when Hello packets are received and then a new neighbor can be created. If it is in deny state, the corresponding new neighbor need not be created. Multiple neighbor access lists can be configured (New CISCO bin only allows to configure a neighbor access list; old bin allows to configure multiple neighbor access lists). Once a neighbor is filtered, the neighbor is then denied

Example

The following example shows how to configure **stub multicast routing** on router A and how router B uses access list 1 to filter all PIM information from router A. SwitchA has an egress port vlan8, and the IP address is 10.0.0.1. switchB is a central routing road, the egress port is vlan8, the address is 10.0.0.2

switch A Configuration

switch_config# ip multicast-routing

switch_config#interface vlan8

switch_config_v8#ip address 10.0.0.1 255.255.255.0

switch_config#interface vlan9

switch_config_vlan9# ip igmp helper-address 10.0.0.2

switch B Configuration

switch_config# ip multicast-routing

switch_config#interface vlan8

switch_config_v8#ip address 10.0.0.2 255.255.255.0

switch_config_v8# ip pim-sm nbr-filter 1

switch_config#ip access-list standard 1

switch_config_std# deny 10.0.0.1

switch_config_std# permit any

Related command

ip pim-sm jp-intvl

41.1.13 ip pim-sm nbr-track

Syntax

To forbid the limitation of the JOIN packets globally and enable neighbor tracking, run the following first command:

ip pim-sm nbr-track

no ip pim-sm nbr-track

Parameter

Name	English prompt	Notes
nbr-track	nbr-track -- pim-sm interface neighbor join desire tracking	

Default value

If the global congfigration mode is not configured, neighbor tracking is disabled

Command mode

Interface configuration mode

Usage guidelines

This command is used to forbid the limitation function of the join packets and enable neighbor tracking. In this way, (s, g), (*, g), (s, g, rpt) each downstream will retain the corresponding neighbor (referring to the neighbor that sent the join message), and upstream will retain the corresponding RPF nbr. By default, neighbor tracking

is disabled, and join message suppression capability is allowed. Only when all neighbors on the port support nbr track, the neighbor tracking capability will take effect, and the corresponding flag bit of the pim-sm port structure will be set

Example

The following example sets the DR priority value to 200 for the interface vlan8:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm nbr-track

Related command

None

41.1.14 ip pim-sm override

Syntax

The (s, g) or (*, g) upstream port receives the prune message, but the local is still in the join desire state, then an OT timer with a time interval of RANDOM (override-intvl) is triggered locally. After the timer expires, the local will send a join message to the upstream RPF neighbor. The time is negotiated based on the delay-intvl in the neighbor hello message

ip pim-sm override *override-intvl*

no ip pim-sm override

Parameter

Name	English prompt	Notes
override	Override -- pim-sm override timer	
override-intvl	<0-65535> -- override_interval((uint: ms, default: 2500)	

Default value

2.5s

Command mode

Interface configuration mode

Usage guidelines

The finally calculated prune deny time is based on the maximum value among all the values reported by all neighbors. If some neighbor does not support prune deny, the default value is selected. If OT is enabled, the value can be random. If the interval of the prune deny timer is locally set, it will be reported to upstream neighbors through the HELLO packets

Example

The following example sets the override value to 2000 ms for pim-sm interface vlan8 configuration:

switch_config#interface vlan8

switch_config_v8#ip address 10.0.1.2 255.255.255.0

switch_config_v8#ip pim-sm override 2000

Related command

ip pim-sm lan-delay

41.1.15 router pim-sm

Syntax

To enter the global PIM-SM view, under which there is common attributes, run the following first command:

router pim-sm [vrf *vrf_name*]

no router pim-sm [vrf *vrf_name*]

Parameter

Name	English prompt	Notes
pim-sm	pim-sm --Enable global PIM sparse protocol configure status	
vrf	vrf -- VPN Routing/Forwarding Instance	
vrf_name	WORD -- VPN Routing/Forwarding Instance name	

Default value

The system will not generate the PIM-SM view by default

Command mode

Global configuration mode

Usage guidelines

If the router pim-sm command is configured globally or the PIM-SM related configuration is first configured on the port, the global PIM-SM view will be created. If there is some PIM-SM related configuration on the port, the global view cannot be deleted

Example

The following command shows how to create the global PIM-SM view:

switch_config#router pim-sm

switch_config_ps#

switch_config#router pim-sm vrf mxw

switch_config_ps_(mxw)#

Related command

ip pim-sm

41.1.16 hello-option

Syntax

To configure in the global PIM-SM view, the global DR priority, the prune delay time, the transmission interval of HELLO packets, the prune deny time, neighbor tracking and neighbor timeout time, run the following command:

hello-option { dr-pri *pri-value* **/lan-delay** *delay-intvl* **/**

override *override-intvl* **| nbr-track | holdtime** *hold-intvl* **}**

no hello-option {dr-pri /lan-delay /override | nbr-track | holdtime }

Parameter

Name	English prompt	Notes
dr-pri	dr-pri -- PIM-SM global DR priority	
pri-value	<0-4294967295> -- DR priority, preference given to larger value	If this command is not configured, the default DR priority of this process is 1
lan-delay	lan-delay --pim-sm prune delay	Configures the prune delay time
delay-intvl	<0-32767> -- lan delay(uint: ms, default: 500)	The default prune delay time is 500ms Unit: 100ms Only 15 bits, the 16th bit is T bit
override	override -- pim-sm override timer	Configures the prune deny
override-intvl	<0-65535> -- override_interval((uint: ms, default: 2500)	The default prune deny time is 2500ms. Unit: 100ms
nbr-track	nbr-track -- pim-sm interface neighbor join desire tracking.	If this command is configured, the JOIN packets will not be limited
holdtime	holdtime -- keep alive time to neighbor	
hold-intvl	<4-65535> -- keep alive time value(uint: s, default: 3.5x hlo_intvl)	In normal case, its value is 3.5 times larger than the Hello interval on a port. The default neighbor holdtime is 105 seconds.

Unit: s

Default value

See the table above

Command mode

Global PIM-SM view

Usage guidelines

If there is no corresponding configuration items on a port, the globally configured attributes will be used as the corresponding attributes on the port. The change of the global DR priority may affect the new DR selection

The rules of DR selection are shown below:

1. The highest DR priority on a port will be selected as the DR of the network segment to which this port belongs; if there are many same DR values, the relatively large IP address among the main IP address on the local port and the main IP address of the neighbor will be selected as DR

2. If there are neighbors on a port or the DR priority is not supported on a port, the relatively large mainaddress will serve as DR

Note:

If the port DR becomes non-DR or vice versa, it may be necessary to comprehensively consider the assert state machine and the corresponding actions of (s, g), (*, g), (*, *, rp), and also need to consider whether to notify IGMP v1

Example

The following example sets the DR priority value to 200 for global pim-sm configuration:

switch_config#router pim-sm

switch_config_ps#hello-option dr-pri 200

41.1.17 accept bsm-adv

Syntax

You can run **accept bsm-adv** in global mode to set the filtration list. The filtration list settings is especially for filtrating specific BSM source addresses and receive the designated BSM source address. To cancel the filtration, you can run **no accept bsm-adv [*list* *std-acl*]**

accept bsm-adv list *std-acl*

no accept bsm-adv list *[std-acl]*

Parameter

Name	English prompt	Notes

accept	Accept -- Acceptable RP filter	
bsm-adv	bsm-adv -- BSM packet source address accept filter	
list	List -- IP access-list for bsm source-list	
std-acl	WORD -- stand access list name	It is used to limit the range of the BSM source address

Default value

This filtration is disabled by default

Command mode

pim-sm global view

Usage guidelines

Only one filtration command can be set

Example

The following example shows that the BSM notifications only from network segment 192.2.2.0/30 can be received

switch_config#router pim-sm

switch_config_ps#accept bsm-adv list adv-src

switch_config_ps#exit

switch_config#ip access-list stand adv-src

switch_config_std#permit 192.2.2.0 255.255.255.252

41.1.18 accept crp-adv

Syntax

To set the filtration list specially for filtrating the address range of specific groups, limiting to receive the C-RP-ADV packets from specific candidate rp unicast, and specifying the group address' range in the received packets through ACL. To cancel the filtration, you can run no form of the command

accept crp-adv A.B.C.D *[std-acl]*

no accept crp-adv A.B.C.D *[std-acl]*

Parameter

Name	English prompt	Notes

accept	accept -- Acceptable RP filter	
crp-adv	crp-adv -- C-RP-ADV accept filter	
A.B.C.D	A.B.C.D -- IP address of candidate RP for group	
std-acl	WORD -- Standard ACL name for group-address	

Default value

Disable (not filtrating C-RP-ADV from c-rp)

Command mode

pim-sm global view

Usage guidelines

After this command is set, BSR only processes C-RP-ADV from RP. Additionally, the range of the group address must be allowed by the standard ACL

Example

The following example states that the switch will accept c-rp messages RP address is 100.1.1.1 for the multicast group 224.2.2.2:

switch_config#router pim-sm

switch_config_ps#accept crp-adv 100.1.1.1 grp-acl

switch_config#ip access-list stand grp-acl

switch_config_std#permit 224.2.2.2 255.255.255.255

41.1.19 accept rp-addr

Syntax

Run **accept-rp** in global configuration mode to set the filtration list to filter the specific group address range, deciding whether the join/prune of (*, G) is acceptable and responding to the registration information of specific destination group addresses. To cancel this setting above, run the "no" form of this command

accept rp-addr A.B.C.D *[std-acl]*

no accept rp-addr A.B.C.D *[std-acl]*

Parameter

Name	English prompt	Notes
accept	accept -- Acceptable RP filter	

rp-addr	rp-addr -- RP address accept filter	
A.B.C.D	A.B.C.D -- IP address of RP for group	
std-acl	WORD -- ip stand access-list name for group	If omit it, switch will process all the PIM-SM message to any group which is mapped to the RP

Default value

Disable (All Join, Prune or Register packets will be processed)

Command mode

pim-sm global view

Usage guidelines

After this command is set, the router processes only those Join packets which are mapped to the designated RP. Another point deserving attention is that the range of the group address must be allowed by the standard access list. The aggregation point of the corresponding group must be the calculated RP, and when the aggregation point matches up with the RP can the access filtration list be applied. If the group address is denied, RP will reject the Join and Register packets; after the Register packets are received, RP will return a Register Stop packet to the registration packet generator

This command can be set many times if the rp-addr parameters in this command are different. If the RP that the group address is mapped to is not in the configured range, the RP will be denied directly

Example

The following example states that the switch will accept join or prune messages destined for the RP at address 100.1.1.1 for the multicast group 224.2.2.2:

switch_config#router pim-sm

switch_config_ps#accept rp 100.1.1.1 no-ssm-range

switch_config#ip access-list extended no-ssm-range

switch_config_std#permit 224.2.2.2

%PIM-6-INVALID_RP_JOIN: Received (*, 238.1.1.1) Join from 192.17.20.173 for invalid RP 1.1.1.1

switch#show ip mroute

(*, 238.1.1.1), 00: 02: 52/00: 00: 07, RP 1.1.1.1, flags: S

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

v8, Forward/Sparse, 00: 02: 52/00: 00: 07

It can be seen that the previous address, *.238.1.1.1, ages after the filtration is set

41.1.20 accept register

Syntax

When the Register range list is set on C-RP, the selection is RP and the PIM-SM Register packet is received, the filtration list should be used to filter the Register packets. In this case, you should run **accept-register**, and if you want to cancel the filtration, run the "no" form of this command

accept register {**list** *ext-acl* | ***route-map*** *map-name*}

no accept register [**list** *ext-acl* | ***route-map*** *map-name*]

Parameter

Name	English prompt	Notes
accept	accept -- Acceptable RP filter	
register	register -- Registers accept filter	
list	list -- standard access list	
ext-acl	WORD -- IP access-list name for register source	
route-map	route-map -- route map	
map-name	WORD -- route map name	

Default value

The access list filtration or the route-map filtration will not be conducted to the Register packets

Command mode

pim-sm global view

Usage guidelines

This command is used to prevent those unauthenticated data source from sending the Register packets to RP. If an unauthenticated data source sends a Register packet to RP, RP will return a Register Stop packet at once. This command takes effect only on the machine that runs as RP

Example

The following example shows how to restrict the RP from allowing sources in the Source Specific Multicast (SSM) range of addresses to register with the RP

switch_config#router pim-sm

switch_config_ps#accept register list no-ssm-range

switch_config#ip access-list extended no-ssm-range

switch_config_std#deny ip any 232.0.0.0 0.255.255.255

switch_config_std#permit ip any any

Related command

reg-src

41.1.21 anycast-rp

Syntax

Through configuring **anycast-rp** and the corresponding neighbor address, you can specify the corresponding peer neighbor to share the load of RP. To cancel this setting above, run the "no" form of this command

anycast-rp A.B.C.D nbr A.B.C.D

no anycast-rp A.B.C.D nbr A.B.C.D

Parameter

Name	English prompt	Notes
anycast-rp	anycast-rp -- anycast rp for pim-sm	
A.B.C.D	A.B.C.D -- anycast rp address	
nbr	Nbr -- anycast rp neighbor	
A.B.C.D	A.B.C.D -- anycast rp neighbor address	

Default value

This command takes no effect by default

Command mode

pim-sm global view

Usage guidelines

PIM-SM only regulates the standards of the single RP, but a big data flow can cause single RP overload easily. In this case, this command will be used to solve the overload of RP in the PIM-SM domain

Note:

1.You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the mute terminal router that connects other PIM equipments in the PIM domain through dial-up

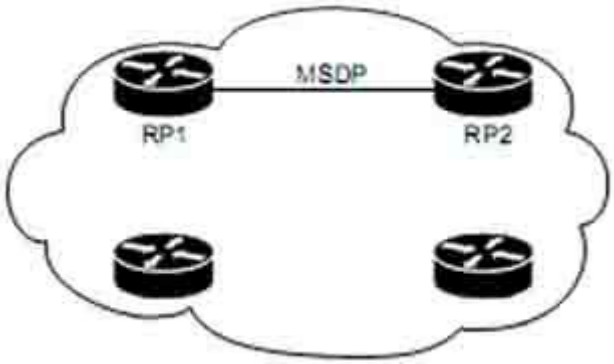
2.If the inside-domain MSDP is not used, the machine that specifies **anycast rp** must at the same time specify the address of a neighbor with the same RP address so as to facilitate the processing of the register

3.The command, **anycast-rp A.B.C.D nbr**, is used on those devices that have no MSDP settings and provide an address as the static RP. All peer neighbors need be specified. The neighbors are reachable to one another

4.If MSDP is set, the device, if it has provided the static RP address, need not specify **anycast rp nbr**

Example

1. The following example shows how to set the anycast-rp address when MSDP is used



SP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
I
ip msdp peer 10.1.1.2 connect-source loopback 1
ip msdp originator-id loopback 1

SP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
I
ip msdp peer 10.1.1.1 connect-source loopback 1
ip msdp originator-id loopback 1
Designate the static RP address on other devices, for example, do it on router Sa:
Sa:
router pim-sm
static-rp 10.0.0.1

2. The following example shows how to make settings when the MSDP is not used

SP1:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255

ip pim-sm
Interface loopback 1
ip address 10.1.1.1 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1

SP2:
Interface loopback 0
ip address 10.0.0.1 255.255.255.255
ip pim-sm
Interface loopback 1
ip address 10.1.1.2 255.255.255.255
router pim-sm
anycast-rp 10.0.0.1 nbr 10.1.1.1
anycast-rp 10.0.0.1 nbr 10.1.1.2
static-rp 10.0.0.1
Designate the static RP address on other devices, for example, do it on router Sa:
Sa:
router pim-sm
static-rp 10.0.0.1

Related command

None

41.1.22 reg-rate-limit

Syntax

As to (s, g), if you want to set the regeneration rate limit of the PIM-SM registration packets per second, you should use the **reg-rate-limit** command; to cancel this settings, you can run **no reg-rate-limit [*rate*]**

reg-rate-limit *rate*

no reg-rate-limit *[rate]*

Parameter

Name	English prompt	Notes
reg-rate-limit	reg-rate-limit -- Rate limit for data register packets	
rate	<1-65535> -- Packets per second	

Default value

The regeneration rate of the registration packets of any (s, g) can be limited to one packet per second

Command mode

pim-sm global view

Usage guidelines

This command can be used to limit the regeneration rate of registration packets of (s.g) on the DR router. After this command is enabled, the load of the DR router will be limited. At the initial establishment of multicast path, the sudden eruption of large traffic of the multicast source may lead to packet loss due to the rate limit and the multicast receiver cannot receive all the multicast packets

Example

The following example shows how to do the corresponding settings to let each (s.g) generate two registration packets per second

switch_config#router pim-sm

switch_config_ps#reg-rate-limit 2

41.1.23 reg-src

Syntax

To specify an IP address of a port to run as the source address for DR to transmit the PIM-SM registration packets, replacing the default port's address that connects the data source, run **reg-src**. If you use the **reg-src** command, the specified port must be active. To cancel this settings, you can run **no reg-src**

reg-src *intf-type intf-number*

no reg-src [*i*ntf-type *intf-number*]

Parameter

Name	English prompt	Notes
reg-src	reg-src -- Source address used by register packets	
intf-type intf-number	Type of the designated port and its name	If a port has no main IP address or has no ID, the settings will take no effect The L3 protocol of a designated port must be up

Default value

By default, the port that connects DR and the data source will be used as the source address of the Register

packet to conduct packet encapsulation

Command mode

pim-sm global view

Usage guidelines

When the default source address of the Register packet is not the only routable destination address for RP to return the Register Stop packet, you should use this command to set a new source address for the Register packet. For example, in cases that the source address of the Register packet will be filtered on RP by ACL or the source address is not the only IP address, the Register Stop packet returned by RP may not reach the corresponding DR correctly and then the PIM-SM registration finally may fail

If the source address of the Register packet is not specified or the specified source address takes no effect, DR will choose the port, which connects the data source, as the source address of the Register packet. Therefore, it is recommended to set for the PIM-SM domain a unique routable address on the loopback port as the source address of the Register packet

Example

The following example shows how to designate the address of the loopback3 port of DR as the source address of the Register packet

switch_config#router pim-sm

switch_config_ps#reg-src loopback 3

41.1.24 spt-threshold

Syntax

For a specific group, the service message flow will switch to the shortest path tree after reaching the configured threshold. In the pim-sm configuration mode, use the command **spt-threshold** to configure the leaf nodes of PIM-SM. Use the no form of the command to restore the default value of switching to SPT

spt-threshold {**infinity**/***kbps***} [*stand-acl*]

no spt-threshold {**infinity**/***kbps***} [*stand-acl*]

Parameter

Name	English prompt	Notes
spt-threshold	spt-threshold -- Threshold of source-tree switching	
infinity	Infinity -- Never use source-tree	
kbps	<0-4294967> -- Data packet rate in pkt/s	
stand-acl	WORD -- ip standard access list name for group	

Default value

There is no traffic limit for switchover. When the downstream receiver tries to join the data source, the data source will switch over to the SPT forwarding when it receives the data

Command mode

pim-sm global view

Usage guidelines

If the forwarding rate of a multicast source reaches or exceeds the designated threshold, the leaf node will send a (s, g) Join packet to the multicast source for constructing the source tree—the shortest path tree

If the threshold is set to infinity, all multicast sources for the designated group take the sharing tree for packet forwarding. The group access list designates which groups use the configured threshold for SPT switchover. If the message flow from the data source is less than the designated threshold, the PIM-SM router of the leaf node will be switched back to the sharing tree after a period of time and then send the Prune message to the source tree

Example

The following example sets a threshold of 4 kbps, above which traffic to a group from a source will cause the switch to switch to the shortest path tree to that source:

switch_config#router pim-sm

switch_config_ps# spt-threshold 4

Related command

None

41.1.25 ssm

Syntax

To set the range of a specific multicast group, run **ssm** command. To cancel the designated SSM range, run **no ssm**

ssm {**default** | **range** *std-acl*}

no ssm [**default** | **range** *std-acl*]

Parameter

Name	English prompt	Notes
ssm	ssm -- Configure Source Specific Multicast group range	
Default	default -- Use default group range(232/8) for SSM mode	
Range	range -- Group range ACL used for SSM	
std-acl	WORD -- IP named access-list	

Default value

disable

Command mode

pim-sm global view

Usage guidelines

When PIM-SM is enabled, the default or configured range of the multicast group address can be used. If the multicast group is in the designated SSM range, the locally corresponding (*, g) must be canceled. This requires the same strategic SSM shall be set in the whole PIM-SM

Note:

The same SSM strategy shall be set in the whole PIM-SM, otherwise the configured SSM will take no effect on preventing (*, g) Join for IGMPv3 can also specify the addition of (s, g) Join. Additionally, the (*, g) collision may be caused

PIM-SM cannot be used together with other protocols. The configuration of SSM prevents the transmission of (*, g) Join and (*, *, rp) Join, and the PMBR device cannot send specific (s, g) Join to the upstream devices

After SSM is set, MSDP cannot generate or receive SAs belonging to the designated range of the multicast group address. Our solution is that MSDP notification will be omitted if the group in the (S, G) items of PIM-SM is in the designated SSM group range

If the group range covers BIDIR group range, the previous configuration will be kept, and display error message to the later (not support now)

Example

The following example shows how to configure SSM service for the IP address range defined by access list 4:

switch_config#router pim-sm

switch_config_ps# ssm range grp_range

switch_config#ip access-list stand grp_range

switch_config_std# permit 224.2.151.141

Related command

None

41.1.26 c-bsr intf_type intf_name

Syntax

To set a router to be a candidate BSR router, run the first of the following two commands; to cancel this settings, run the second one of the following two commands

c-bsr *[intf_type] [intf_name]* [*hash-length* [*priority*]]

no c-bsr *[intf_type][intf_name]*

Parameter

Name	English prompt	Notes
c-bsr	c-bsr -- Candidate bootstrap router (CBSR)	
intf-type intf-number	Type of the designated port and its name	
hash-length	<0-32> -- Hash Mask Length used by RP selection	Specify the length of the hash mask.
priority	<0-255> -- Priority value used by BSR election	BSR election priority

Default value

Dynamic BSR selection is disabled

Command mode

pim-sm global view

Usage guidelines

After this command is set, the designated address of a port will be used as the BSR address and it will send BSM (bootstrap messages) to all PIM-SM neighbors on the local machine. Each neighbor will compare the previously received BSM with the currently received BSM, and if the BSR address in the current BSM is larger than or equal to that in the previously received BSM, the locally stored BSM will be updated and the current BSM will be forwarded; otherwise, the current BSM will be dropped directly. Before the candidate BSR receives the BSM with higher priority, it always regards itself as the BSM router in the corresponding management domain

Note:

You'd better configure this command on the equipment with good connectivity in the PIM domain in the backbone network. That is, this command is not suitable to be set on the mute terminal router that connects other PIM equipments in the PIM domain through dial-up

On accepting C-RP-Adv, BSR only accepts those contents that satisfy the SZ range; if the content exceeds the SZ range, it will be omitted

You can specify only one port of a device as the BSR address; if multiple commands are set, the previously configured candidate BSRs will be replaced

The condition for this command to be effective is that the IP address of the designated port is in PIM-SM state and the protocol is up

Example

The following example configures the IP address of the switch on Ethernet interface 0 to be a candidate BSR with priority of 10:

switch_config# router pim-sm

switch_config_ps# c-bsr vlan8 10 100

Related command

c-bsr admin-scope {global |gaddr gmask} [hash-length] [priority]

41.1.27 c-bsr admin-scope

Syntax

To set a candidate BSR in the administration domain, run the first one of the following two commands.

c-bsr admin-scope {**global** | *gaddr gmask*} [*hash-length* [*priority*]]

no c-bsr *admin-scope* {**global** | *gaddr gmask*} [*hash-length* [*priority*]]

Parameter

Name	English prompt	Notes
c-bsr	c-bsr -- Candidate bootstrap router (CBSR)	
admin-scope	admin-scope -- pim-sm administrator scope	
global	Global -- global group range	224.0.0.0/255.0.0.0
gaddr	A.B.C.D -- sz range, private group address prefix	239.0.0.0 to 239.255.255.255
gmask	A.B.C.D -- private group mask	
hash-length	<0-32> -- Hash Mask Length used by RP selection	
priority	<0-255> -- Priority value used by BSR election	

Default value

The global domain is 224.0.0.0/4 by default

Command mode

pim-sm global view

Usage guidelines

This command is used to set the candidate BSR in the administration domain. This command corresponds to the admin-scope command in the domain boundary and is used to specify the range of the administration domain

Note:

If the command c-bsr intf type intf name is not configured, this command takes no effect

It is recommended to set this command in the administration range (239.0.0.0~ 239.255.255.255)

Example

The following example shows that C-BSR only takes effect in the administration domain 239.1.1.0/24:

switch_config# router pim-sm

switch_config_ps#c-bsr vlan8 10 250

switch_config_ps#c-bsr admni-scope 239.1.1.1 255.255.255.0

Related command

c-bsr intf_type intf_name [hash-length [priority]]

41.1.28 bsm-policy

Syntax

To set the BSM reception policy, run the first one of the following two commands in PIM-SM configuration mode. To resume the default settings, run the other command.

bsm-policy { unicast {rcvd | send}/**forward-all | backward}**

no bsm-policy { unicast **{rcvd | send} /**forward-all }

Parameter

Name	English prompt	Notes
bsm-policy	bsm-policy -- PIM-SM RP-address (static RP)	
unicast	"unicast -- unicast bsm packet	The default value allows the reception of the unicast BSM packets. The backward compatibility supports the transmission of unicast BSM
rcvd	Rcvd -- permit to receive bsm unicast message	
send	Send -- permit to send bsm unicast message(backward compatible)	
forward-all	forward-all -- forward all bsm packet"	The horizontal division port will not forward all BSM packets, including unicast or no-forward-bit reset packets

Default value

There is no BSM reception or transmission policy

Command mode

pim-sm global view

Usage guidelines

Refer to the description of this command

Example

The following example configures the local switch can receive bsm unicasted from neighbor:

switch_config# router pim-sm

switch_config_ps# bsm-policy unicast rcvd

Related command

None

41.1.29 static-rp

Syntax

To set the static RP of PIM-SM, run the first one of the following two commands; to resume the default settings, run the other command.

static-rp *rp-addr* [*std-acl*] [**override**]

no static-rp *rp-addr* [*std-acl*] [**override**]

Parameter

Name	English prompt	Notes
static-rp	static-rp -- PIM-SM RP-address (static RP)	
rp-addr	A.B.C.D -- IP address of RP"	
std-acl	WORD -- IP access-list"	
override	Override -- Overrides RP-mapping information by BSR	When static RP goes against dynamic RP, if the parameter is not designated, the dynamic RP will be chosen first, and if no dynamic RP exists or dynamic RP takes no effect can static RP take effect

Default value

Disable

Command mode

pim-sm global view

Usage guidelines

The designated IP address of static RP must be legal unicast address and cannot be the loopback address (127.0.0.0/8). If ACL is designated, the configured static RP will serve the matched multicast group; if ACL is not designated, the configured static RP will serve all multicast groups (224.0.0.0/4). When static RP goes against dynamic RP, the former will be first chosen

In PIM-SM or BIDIR mode, each group will be provided with an RP. All routers in the same administration domain must follow the identical rule to set RP for the group. RP can be obtained through two mechanisms: static configuration of the RP address or the BSR mechanism's dynamic learning of RP address. The static rp-address command can be used to set an RP to be the aggregation point of multiple groups. The ACL configured by static RP defines the RP application range. If the standard ACL is not set, the designated static RP will be applied to all groups. One PIM router can use multiple RPs, but it can use the only RP for a specific group

If multiple static rp-address commands are set, the matchup rules of group-to-rp are listed below:

If a group matches up with multiple static RP rules, suitable RPs can be chosen according to the longest matchup principle specified by the standard ACL. As to the static configuration without designated ACL, it can be applied to all groups, but the entries in the ACL must be first set

If a group and multiple ACLs accord to the longest matchup principle, the IP addresses of RPs must be compared and those RPs with big IP addresses come prior in choice

If the static RP configuration is adopted, the reachability test will not be conducted to the designated RP. If an RP is selected, the RP with a comparatively low RP will not be chosen even though the route of the selected RP does not exist locally

Each command can be used to specify a static RP address. If the designated static RP address or ACL rule is same during configuration, the new configuration will replace the previous configurations

In case static RP and dynamic RP are used together, the rules of group-to-rp are listed below:

When the override is not specified, the RPs, dynamically learned through the BSR mechanism, come prior to static RPs

If dynamic RP is used, the c-rp intf_type intf_name command must be set

Note:

The same RP cannot be used simultaneously on BIDIR and PIM-SM

The statically configured RP only supports global SZ or provides support even if global SZ has not yet created

Example

The following example shows how to designate 198.92.37.33 to be the static RP address

switch_config#router pim-sm

switch_config_ps#static-rp 198.92.37.33

Related command

c-rp intf_type intf_name

41.1.30 c-rp intf_type intf_name

Syntax

To set a port to be C-RP and to send the unicast notification periodically to a designated BSR router in the PIM-SM domain, run the first one of the following two commands. To resume the default settings, run the other command

c-rp *intf-type intf-name* [**list** *std-acl*] [**pri** *pri-value*]

no c-rp *intf-type intf-name* [**list** *std-acl*] [**pri**]

Parameter

Name	English prompt	Notes
c-rp	c-rp -- Candidate RP router (CRP)	
intf-type intf-name	Designating the interface type and the interface's nam. The IP address of the port will be advertised as a c-rp address.	PIM-SM must be enabled on C-RP
list	list -- IP access-list for group-list	It is the prefix of the group address
std-acl	WORD -- access list name	
pri	pri -- priority of rp address	
pri-value	<0-255> -- priority of rp address candidate	The smaller the value is, the higher the priority is. The default value is 192

Default value

Dynamic RP selection is disabled

Command mode

pim-sm global view

Usage guidelines

This command is used to notify all BSRs on C-RP. The range of the group address is listed in a form of the standard ACL

Note:

PIM-SM must be enabled on the port that serves as C-RP

You'd better set C-RP on the main PIM-SM domain to avoid static configuration on similar routers or the on-demand dialup stub routers

If C-RP is not specified with a multicast group range, C-RP will serve all multicast groups

If you want to set a router to be C-RP for multiple group ranges, you need to represent multiple group ranges with multiple rules when configuring STD-AC1 that group-list corresponds to

One port can only be set to one C-RP and the following configuration will replace the previous configuration, including the replacement of STD-AC1

You can set C-RP for multiple ports on the same PIM-SM router

Multiple C-RPs can use the same standard ACL

If this command is run many times on a same interface, the previous configuration will be replaced

If multiple SZs are known on C-RP, unicast C-RP-Adv will be sent to the BSR of each SZ. It is noted that the established group range cannot exceed the group range of the destination SZ

If C-RP itself is the ZBR of an SZ, the Admin Scope Bit in the C-RP-Adv packet must be reset; otherwise, this bit will not be reset. At present, it is used for BSR to record logs but possible to be used for protocol expansion

Example

The following example shows how to designate lo172 and lo173 to be C-RP ports, the former limiting to provide RP to the group of prefix 239.1/16

switch_config#router pim-sm

switch_config_ps# c-rp loopback172 group-list grp-range

switch_config# ip access-list standard grp-range

switch_config_std# permit 239.1.0.0 255.255.0.0

switch_config_ps# c-rp loopback173

Related command

None

41.1.31 intvl-time

Syntax

To enable the periodical transmission of join/prune packets and set the interval of periodically transmitting the Hello, BSM or C-RP-Adv packets, run the first of the following two commands:

intvl-time { **join-prune** *jp-intvl* | **hello** *hlo-intvl* | **c-bsr** *cbsr-intvl* | **crp-adv** *crp-intvl* | **spt-check** spt-intvl }

no intvl-time { **join-prune** | **hello** | **c-bsr** | **crp-adv** | **spt-check** }

Parameter

Name	English prompt	Notes
intvl-time	intvl-time-- regular message generate timer interval	
join-prune	join-prune-- pim-sm join/prune message interval	
jp-intvl	<1-65535>-- value for timer (unit: s)	The default interval of transmitting Join/Prune packets is 60 seconds
hello	hello-- pim-sm hello advertisement interval	Sets the interval of transmitting the Hello packets
hlo-intvl	<1-65535>-- periodic pim hello message are sent(unit: s)	The default interval of transmitting Hello packets is 30 seconds
c-bsr	c-bsr-- Candidate bootstrap router (candidate BSR)	

cbsr-intvl	<10-65535>-- periodic pim bsm message are sent(unit: s, default: 60)	The default interval of self-selecting packets is 60 seconds
crp-adv	crp-adv-- pim-sm C-RP-ADV interval	Sets the interval of transmitting the C-RP-Adv packets
crp-intvl	<1-65535>-- periodic pim CRP-ADV message are sent(unit: s, default: 60)	The default interval of transmitting Report packets is 60 seconds
spt-check	spt-check-- spt switch response time interval(uint: 100ms)	
spt-intvl	<1-65535>-- spt switch response time interal(uint: 100ms, default: 2s)	

Default value

See the above-mentioned table

Command mode

pim-sm global view

Usage guidelines

If the holdtime of Join-prune packet is not set and the Join packets from the downstream neighbor have not been received in three JP timeout periods, the downstream that corresponds to the multicast entry will be shifted to the prune state. The default holdtime is 3 minutes. The interval in port configuration mode is prior to the join/prune interval in global mode. The relevant interval and holdtime entries have certain time matching requirements

When using the no form of the command, the specific time parameters required to be input will not be checked and will be restored to the corresponding default values

Example

The following example sets the join/prune advertisement interval value to 30 for global pim-sm configuration:

switch_config#router pim-sm

switch_config_ps# intvl-time join-prune 30

Related command

holdtime

41.1.32 holdtime

Syntax

To set the interval of the timeout timer of PIM-SM, run the first one of the following two commands. To resume the default settings, run the other command

holdtime {join-prune *jp-hold* **| assert** *asrt-hold* **| c-bsr** *cbsr-hold* **| crp-adv** *crp-hold* **| sz** *sz-hold***}**

no {join-prune *jp-hold* **| assert** *asrt-hold* **| c-bsr** *cbsr-hold* **| crp-adv** *crp-hold* **| sz** *sz-hold***}**

Parameter

Name	English prompt	Notes
holdtime	holdtime-- holdtime for keep the status	
join-prune	join-prune-- pim-sm join/prune statue holdtime	
jp-hold	<1-65535>-- join/prune status keep alive value for timer (unit: s; default, 210)	The default value is 210 seconds.
assert	assert-- assert status keep alive time	
asrt-hold	<7-65535>-- periodic pim hello message are sent(unit: s, default 180)	The default value is 180 seconds.
c-bsr	c-bsr -- BSR status keep alive time	
cbsr-hold	<1-65535> -- periodic pim bsm message are sent(unit: s, default: 130)	By default, it is as follows: holdtime timeout time= holdtime's interval*2+10 By default, the holdtime's interval is 60 seconds and the holdtime's timeout time is therefore 130 seconds.
crp-adv	crp-adv -- pim-sm C-RP-ADV keep alive time	
crp-hold	<1-65535> -- CRP-ADV message alive time intvl(unit: s, default: 150)	The default value is 150 seconds. Because non-BSR updates its timeout time through the BSR's holdtime packets, the timeout time of C-RP must not be less than the interval of holdtime packet transmission. It is best when the former is 2.5 intervals or beyond.
sz	sz -- scope zone keep alive time	The default value is 1300 seconds.
sz-hold	<10-429496729> -- scope zone keep alive time value(unit: s, default: 1300)	

Default value

See the above-mentioned table

Command mode

pim-sm global view

Usage guidelines

If the holdtime is set on a port, first comes the configuration of this port and then the global configuration; finally, if neither configuration is done, the default configuration will be chosen

When using the no command, the specific time parameters required to be input will not be checked and will be restored to the corresponding default values

Note:

When configuring the holdtime of C-RP, you should set the timeout time of C-RP to 2.5 holdtime transmission intervals or beyond to prevent the C-RP loss in the BSR holdtime packet

The timeout time of SZ must be longer than the BSR timeout time and you'd better set it to be 10 times of BSR timeout

Example

The following example shows how to set the holdtime of C-RP to 150 seconds, among which C-RP and C-BSR are not set on Ra

Ra_config# router pim-sm

Ra_config_ps# holdtime c-rp 200

Related command

intvl-time

41.1.33 log

Syntax

To enable the log switch to record DR's change, neighbor's up or down, address conflict and abnormal packets, run the first one of the following two commands:

log { nbr-change | ipaddr-conflict | pkt-conflict }

no log ***{ nbr-change | ipaddr-conflict |*** **pkt-*** ***conflict }***

Parameter

Name	English prompt	Notes
log	log -- To log conflict	
nbr-change	nbr-change -- neighbor up/down or DR changes	
ipaddr-conflict	ipaddr-conflict -- secondary ip address is conflict with the another neighbor	
pkt-conflict	pkt-conflict -- pim-sm mroute items conflict in the pim-sm pkt	

Default value

The log function is disabled

Command mode

pim-sm global view

Usage guidelines

If there is the log server, the corresponding logs will be recorded to the log server

Example

The following example configures the switch to log the conflict when the exist secondary ip address is also contained in hello packet when receivd from another neighbor

switch_config_ps# log nbr-change

Related command

None

41.1.34 clear ip pim-sm rp-mapping

Syntax

To clear pim-sm RP mapping table information, run the following command

clear ip pim-sm rp-mapping [A.B.C.D]

Parameter

Name	English prompt	Notes
pim-sm	pim-sm-- PIM sparse mode	
rp-mapping	rp-mapping-- Clear RP-mapping table by BSR	
A.B.C.D	A.B.C.D -- RP address	

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to clear rp mapping table

Example

None

41.1.35 clear ip mroute pim-sm

Syntax

To clear ip multicast route pim-sm, run the following command

clear ip mroute pim-sm *

clear ip mroute pim-sm gaddr [saddr]

Parameter

Parameter	Description	Notes
pim-sm	pim-sm -- PIM sparse mode	
*	* -- Delete all PIM-SM multicast routes	
gaddr	A.B.C.D-- Delete the related Group multicast route	
saddr	A.B.C.D-- Delete the related Source multicast route	

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to clear ip multicast route pim-sm

Example

None

41.1.36 show running-configure

Syntax

To display the global PIM-SM information and the main configuration information about a port, run the following command:

show running-config

Parameter

None

Default value

None

Command mode

Other modes except the user mode

Usage guidelines

According to the output information, you can check the configuration information about the current PIM-SM

Example

None

41.1.37 show ip pim-sm bsr-router

Syntax

To display pim-sm BSR information, use the command **show ip pim-sm bsr-router**. The output content includes the elected BSR information and the locally configured candidate RP announcement information

show ip pim-sm bsr-router

Parameter

Parameter	Description	Notes
pim-sm	pim-sm -- PIM Sparse mode	
bsr-router	bsr-router -- display PIM-SM bootstrap (BSR) information	

Default

None

Command mode

Other modes except the user mode

Usage guidelines

None

Example

Output of the command **show ip pim-sm bsr-router**:

```
switch #show ip pim-s bsr
PIMv2 BSR information:
I am BSR in sz 224.0.0.0/4
```

```
CBSR-STM state (0-c, 1-p, 2-e): 2.
Address of BSR:              172.1.1.172
BSR Priority:                64
Hash Mask Length:            30
Uptime:                      05: 18: 00
BSR will expires in 00: 00: 13
Candidate-RP:    173.1.1.173(Loopback173)
Interval of Advertisements:    60 seconds
Next Advertisement will be sent in 00: 00: 07
```

Definitions of domains above:

Domain	Description
sz	Current management domain scope
CBSR-STM state	Current local BSR status
Address of BSR	BSR address in the current domain
BSR Priority	BSR priority
Hash Mask Length	Length of the hash mask advertised by the BSR
Uptime	Survival time of BSR
BSR will expires	BSR timeout remaining time
Candidate-RP	Local candidate C-RP address
Interval of Advertisements	C-RP-ADV periodic notification interval
Next Advertisement	Timeout interval before the next notification

41.1.38 show ip pim-sm sz-info

Syntax

To show pim-sm sz information, including the range of sz, bsm packet number in sz, szt overtime, and the remaining time of BSM is forwarded from iif interface

show ip pim-sm sz-info

Parameter

Parameter	Description	Notes

Parameter	Description	Notes
pim-sm	pim-sm -- PIM Sparse mode	
sz-info	sz-info -- display PIM-SM sz information	

Default value

None

Command mode

Other modes except the user mode

Usage guidelines

The command is used to show pim-sm scope zone information

Example

Output examples of the command **show ip pim-sm sz-info**:

```
switch#show ip pim-sm sz-info
PIMv2 administor scope information:
sz range:    224.0.0.0/4
   group range numbers: 1
   BSM pkt numbers: 0, in current forward queue
   szt not create, for we are c-bsr or BST not expire for no-cbsr
switch #
```

Definitions of domains above:

Parameter	Description
sz range	sz range
group range numbers	group range numbers in sz

41.1.39 show ip pim-sm interface

Syntax

Display pim-sm port related information with the following command

show ip pim-sm interface *[Type number]* [**count**][**detail**]

Parameter

Parameter	Description	Notes
pim-sm	pim-sm-- PIM Sparse mode	
interface	interface-- display PIM-SM interfaces information	
Type number	See interfaces provided by CMD module	(Optional) Interface type and number
count	count -- Number of packets received and sent out the interface	
Detail	detail-- PIM srct of each interface	

Default

None

Command mode

All modes except user mode

Usage guidelines

Output of command **show ip pim-sm interface**:

```
switch#show ip pim-sm interface
Intf          Address              Ver/    Nbr      Hello   DR       DR
                                   Mode    Count    Intvl   Prior    Addr
v8          172.20.21.172          V2/S    0        30      1        172.20.21.172
l174          174.1.1.174          V2/S    0        30      1        174.1.1.174
l173          173.1.1.173          V2/S    0        30      1        173.1.1.173
l172          172.1.1.172          V2/S    0        30      1        172.1.1.172
```

The following command is the output after specifying the count parameter:

```
switch# show ip pim-sm interface count
State:   * - Fast Switched, D - Distributed Fast Switched
         H - Hardware Switching Enabled
Intf          Address              FS      Mpackets In/Out
v8          172.20.21.172          *       59573120/0
l174          174.1.1.174          *       59567488/0
l173          173.1.1.173          *       59568480/0
l172          172.1.1.172          *       59569696/0
```

With the detail parameter, the output example of interface vlan8 is displayed:

```
switch#show ip pim-sm interface vlan8 detail
v8 line protocol is up
  Internet address is 172.20.21.172/24
  Multicast boundary:    not set
  Multicast TTL threshold:    0
  PIM-SM:    enable
  PIM-SM version: 2, mode: sparse
  PIM-SM DR: 172.20.21.172
  PIM-SM neighbor count: 0
  PIM-SM Hello/Query interval: 30
  PIM-SM Hello packets in/out: 0/694
  PIM-SM State-Refresh processing: disable
  PIM-SM State-Refresh origination: disable
  PIM-SM NBMA mode: disable
  PIM-SM domain border: disable
  PIM-SM bsm packet horizon split: disable
```

Definitions of domains above:

Field	Description
Address	Interface IP address of the next hop switch
Interface	Interface type and number that is configured to run PIM
Mode	Multicast mode in which the software is operating
Neighbor Count	Number of PIM-SM neighbors that have been discovered through this interface
Query Interval	Frequency, in seconds, of PIM-SM switch query messages, as set by the ip pim-sm query-interval interface configuration command. The default is 30 seconds
Hello packets In/Out	Number of hello packets into and out of the interface since the switch has been up
Internet address	IP address of the specified interface
Multicast boundary:	Indicates whether an administratively scoped boundary is configured
Multicast TTL threshold:	The time-to-live (TTL) threshold of multicast packets being forwarded out the interface
PIM:	Indicates whether PIM is enabled or disabled
PIM version:	Indicates whether PIM version 1 or version 2 is configured
PIM mode:	Sparse mode

PIM DR:	The IP address of the designated switch (DR)
PIM State-Refresh processing:	Indicates whether the processing of PIM state refresh control messages is enabled
PIM State-Refresh origination:	Indicates whether the origination of the PIM state refresh control messages is enabled
PIM NBMA mode:	Indicates whether the interface is enabled for nonbroadcast multiaccess (NBMA) mode
PIM domain border:	Indicates whether the interface is enabled as a PIM domain border
horizon split	Indicates whether the interface is enabled to retransmit BSM packet

41.1.40 show ip pim-sm neighbor

Syntax

Display pim-sm neighbor information with the following command

show ip pim neighbor [*type number*]

Parameter

Parameter	Description	Notes
Pim-sm	pim-sm -- PIM Sparse mode	
neighbor	neighbor -- display PIM-SM neighbor information	
Type number	See interfaces provided by CMD module	(Optional) Interface type and number

Default

None

Command mode

All modes except user mode

Usage guidelines

According to the output information of this command, the user can see the neighbor information of pim-sm (designated port)

Example

The following is sample output from the **show ip pim-sm neighbor** command:

```
switch#show ip pim-s nei
PIM-SMv2 Neighbor Table
Neighbor          Interface          Uptime/Expires      DR
Address                                                  Prior
172.20.21.173     v8                 00: 00: 08/00: 01: 37   1(DR)
```

Definitions of domains above:

Field	Description
Nbr Addr	IP address of the PIM-SM neighbor
Interface	Interface type and number on which the neighbor is reachable
Uptime	How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table
Expires	How long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table
(DR)	Indicates that this neighbor is a designated switch on the LAN

41.1.41 show ip pim-sm rp

Syntax

Display pim-sm local RP-SET dynamic rp related information with the following command

show ip pim-sm rp [mapping [***rp-address***]| metric [***rp-address***]| all-set]

Parameter

Parameter	Description	Notes
pim-sm	pim-sm -- PIM Sparse mode	
rp	rp -- display PIM-SM RP information	
mapping	mapping -- Displays all group-to-RP mappings	(Optional) Displays all group-to-RP mappings of which the switch is aware (either configured or learned from Auto-RP)
metric	metric -- Displays the unicast routing metric to the RPs	(Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap switch (BSR)
rp-address	A.B.C.D -- IP address of RP	

All-set	all-set -- Displays the whole rp set	

Default value

None

Command mode

All modes except user mode

Usage guidelines

According to the output information of this command, you can see the dynamic rp information in RP-SET

Example

The following is sample output of the **show ip pim-sm rp** command:

```
switch# show ip pim-s rp
GROUP:    227.1.1.1
    RP:    173.1.1.173
    local c-rp


R173_config#show ip pim-s rp
GROUP:    227.1.1.1
    RP:    173.1.1.173
    Uptime/Expires:    06: 21: 49/00: 02: 06
```

The following is sample output of the **show ip pim-sm rp all-set** command:

```
switch# show ip pim-s rp all
sz range: 224.0.0.0/4
  RP-SET node: 224.0.0.0/4
    c-rp: 173.1.1.173(pri: 10)
```

Definitions of domains above:

Field	Decsription
sz range	Scope of management domain sz
RP-SET node	RP-SET corresponding node
Group	Address of the multicast group about which to display RP information
RP	Address of the RP for that group

Local c-rp	This candidate rp is configured locally
Uptime	Length of time the RP has been up (in days and hours). If less than 1 day, time is expressed in hours: minutes: seconds
expires	Time in (hours, minutes, and seconds) in which the entry will expire
Metric Pref	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF)
Metric	Unicast routing metric to the RP announced by the DF
Flags	Indicates the flags set for the specified RP. The following are descriptions of possible flags: C—RP is configured L—RP learned via Auto-RP or the BSR
RPF Type	Routing table from which this route was obtained, either unicast, Distance Vector Multicast Routing Protocol (DVMRP), or static mroute
Interface	Interface type and number that is configured to run PIM-SM

41.1.42 show ip pim-sm rp-hash

Syntax

To calculate and display the rp hash value of the specified group information, use the following command

show ip pim-sm rp-hash *gaddr gmask*

Parameter

Parameter	Description	Notes
pim-sm	pim-sm-- PIM Sparse mode	
rp-hash	rp-hash-- display the RP according to the hash	
gaddr	A.B.C.D-- Displays the RP information for the specified group address	
gmask	A.B.C.D-- Displays the RP information for the specified group mask	

Default value

None

Command mode

All modes except user mode

Usage guidelines

According to the output information of this command, you can see the rp-hash information of the specified group address, including the rp address, priority, and hash value

Example

The output example of the **show ip pim-sm rp-hash** command for group 239.1.1.1:

```
switch#show ip pim-sm rp-hash 239.1.1.1 255.255.255.255
  RP:    173.1.1.173 for 239.1.1.1/0, v2
     Info Source:    173.1.1.173, pri 10, holdtime 150
  PIMv2 Hash Value:
     RP 173.1.1.173, via local BSR, pri 10, hash value 1268904765
```

Definitions of domains above:

Field	Description
RP: 173.1.1.173	Address of the RP for the group specified (239.1.1.1)
Info source: 173.1.1.173	Indicates from which system the switch learned this RP information
holdtime	RP timeout value
via local BSR	Local is the selected BSR
pri	Corresponding priority of rp.
hash value	The calculated hash value

41.1.43 show ip pim-sm anycast-rp

Syntax

To show the current information of anycast-rp, run the following command

show ip pim-sm anycast-rp

Parameter

Parameter	Description	Notes
pim-sm	pim-sm -- PIM Sparse mode	
anycast-rp	anycast-rp -- display register packet rcv and send for anycast-rp	

Default value

None

Command mode

Other modes except the user mode

Usage guidelines

The command is used to show the status of local anycast-rp receiving and sending register packet

Example

Output examples of the command **show ip pim-sm anycast-rp** for group 239.1.1.1:

```
switch# show ip pim-sm anycast-rp
anycast-rp 2.2.2.2 nbr 192.168.18.1 status:    REG_SEND
```

Definitions of domains above:

Parameter	Description
anycast-rp	2.2.2.2 is the address of anycast-rp
nbr	192.168.18.1 is the neighbor address
status: REG_SEND	Forward register packet to the neighbor

41.1.44 show ip pim-sm protocol

Syntax

To show the important information related to pim-sm protocol, run the following command

show ip pim-sm protocol

Parameter

Parameter	Description	Notes
pim-sm	pim-sm -- PIM Sparse mode	
protocol	protocol -- protocol independent multi-cast protocol sparse mode	

Default value

None

Command mode

Other modes except the user mode

Usage guidelines

The command shows information about the current status, port number, neighbor number and received packet number and interval of BSM configuration of pim-sm protocol

Example

Output examples of the command **show ip pim-sm protocol**:

```
switch# show ip pim-sm protocol
PIM-SM is active
pim-sm interface number: 3
pim-sm neighbor number: 1
pim-sm receive pkt num: 133;    bad pkt num: 0
PIM-SM current glb jp_intvl:    60(s)
PIM-SM current glb hello intvl:    30(s)
PIM-SM current glb BSM update timer intvl:    60(s)
PIM-SM current glb crp_intvl:    60(s)
PIM-SM current glb spt_intvl:    2(s)
PIM-SM BSM hold timeout:    130(s)
```

41.1.45 show ip mroute pim-sm

Syntax

Display the pim-sm routing information, you can display the summary information of (s, g) and (*, g), or display the information of the specified item; you can also display the detailed information with status flags

show ip mroute pim-sm [*gaddr /saddr*]**[detail][summary]**

Parameter

Parameter	Description	Notes
pim-sm	pim-sm -- PIM Sparse mode	
gaddr	A.B.C.D -- Group address	
saddr	A.B.C.D -- Source address	

Parameter	Description	Notes
detail	detail-- show pim-sm inner database	
summary	summary-- Displays an abbreviated summary information	

Default value

None

Command mode

All modes except user mode

Usage guidelines

None

Example

1. The following example shows pim-sm routing information:

```
switch# show ip mroute pim-sm 227.1.1.1
IP PIM-SM Multicast Routing Table:

(*, 227.1.1.1)                RP: 173.1.1.173            creat time: 3d02h00m    *G
   Upstream interface:    Null0, rpf' nbr:    0.0.0.0
   ps imm_olist list:
      v8,
      Loopback174,
```

2. The following example shows the summary information of pim-sm routing:

```
show ip mroute pim-s sum
IP PIM-SM Multicast Routing Table summary:
number of (* * RP) entry:    0
number of (* G) entry:    2
number of (s, g) spt entry:    0
number of (s, g) rpt entry:    0

(*, 237.1.1.1)                RP: 175.1.1.173            creat time: 00: 29: 44    *G
   Upstream interface:    Null0, rpf' nbr:    0.0.0.0
   ps imm_olist list:
      v9,

(*, 239.255.255.250)      RP: 175.1.1.173            creat time: 00: 29: 29    *G
```

```
Upstream interface:    Null0, rpf' nbr:    0.0.0.0
ps imm_olist list:
   v8,
```

Definitions of domains above:

Field	Decsription
Upstream interface	RPF upstream interface of the entry
ps imm_olist	Directly receiving port of Pim-sm routing entry
rpf' nbr	Upstream RPF neighbor
creat time	The duration of the entry since it was created

41.1.46 show ip rpf pim-sm

Syntax

Displays the reverse path of pim-sm corresponding to the multicast source address with the following command

show ip rpf pim-sm {*source-address*} [metric]

Parameter

Parameter	Description	Notes
pim-sm	pim-sm -- PIM Sparse mode	
source-address	A.B.C.D -- IP address of multicast source	
metric	metric -- Displays the unicast routing metric	

Default

None

Command mode

All modes except user mode

Usage guidelines

Display specify source address converse forwarding information

Example

Output example of command **show ip rpf pim-sm**:

```
switch#show ip rpf pim-sm 172.1.1.1
PIM-SM:    show ip rpf pim-sm 172.1.1.1
PIM-SM RPF information for 172.1.1.1 :
   RPF_interface:              v8
   RPF_neighbor:                 172.20.21.172
   RPF route/mask(type):    172.1.1.0/24(rip)
```

The output example of the **show ip rpf pim-sm** command with the keyword metric:

```
switch#show ip rpf pim-sm 172.1.1.1 metric
PIM-SM:    show ip rpf pim-sm 172.1.1.1 metric
PIM-SM RPF information for 172.1.1.1 :
   RPF_interface:              v8
   RPF_neighbor:                 172.20.21.172
   RPF route/mask(type):    172.1.1.0/24(rip)
  Metric preference:    120
  Metric:    1
```

Definitions of domains above:

Field	Description
RPF information for source address	Address of the multicast source of interest.
RPF interface	This port is the route egress port to the specified multicast source address, and it is also the port where multicast data arrives
RPF neighbor	Hope to receive the specified multicast source data from the neighbor address.
RPF route/mask	Route to the specified multicast source
RPF type	The route type to reach the specified multicast source (for example, unicast or DVMRP route, static multicast route, etc.)
Metric preference	Administrative distance of dependent routing protocol
Metric	The metric of the current route in the protocol

41.1.47 debug ip pim-sm alert

To display the alert information from mrouting or IP, run the first one of the following two commands

debug ip pim-sm alert

no debug ip pim-sm alert

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

VTY will be exported if the alart information from mrouting or aged (s, g)

41.1.48 debug ip pim-sm assert

Syntax

To track assert messages and state machine information, run the first one of the following two commands:

debug ip pim-sm assert [packet | state- machine | A.B.C.D]

no debug ip pim-sm assert [packet | state- machine | A.B.C.D]

Parameter

Name	English prompt	Notes
state- machine	state-machine -- Trace state machine activity information	
packet	packet -- Trace information about packet	
A.B.C.D	A.B.C.D -- Group address for stm and packet output	

Default value

None

Command mode

EXEC

Usage guidelines

According to the output information, you can check the current assert event of PIM-SM

Result

- Show (S, G) Assert State-machine Actions

- ☐ Show (*, G) Assert Message State Machine actions
- ☐ Show activity after timer timerout
- ☐ Show packet activity

41.1.49 debug ip pim-sm bsr

Syntax

To monitor the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine, run the first one of the following two commands:

debug ip pim-sm bsr[packet | state- machine]

no debug ip pim-sm bsr [packet | state- machine]

Parameter

Name	English prompt	Notes
state- machine	state-machine -- Trace state machine activity information	
packet	packet -- Trace information about packet	

Default value

None

Command mode

EXEC

Usage guidelines

According to the output information, you can check the BSM event of PIM-SM, the C-RP-ADV event or the BSR state machine

Example

None

41.1.50 debug ip pim-sm rp

Syntax

To monitor the related events and packets about PIM-SM-RP-SET change, run the first one of the following two commands:

debug ip pim-sm rp

no debug ip pim-sm rp

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

This command is used to export the reception and transmission of C-RP-ADV and the RP-SET change. As to the change of static RP, no debugging information will be exported at present

Example

None

41.1.51 debug ip pim-sm entry

Syntax

To export the creation and update of (*, *, rp), (*, g), (s, g, rpt) and (s, g, spt) and their simultaneous change of them at the time of RP change, run the first one of the following two commands

debug ip pim-sm entry

no debug ip pim-sm entry

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

According to the output information, you can browse the information about PIMSM creation and update of multicast routing entries

Example

None

41.1.52 debug ip pim-sm event

Syntax

To export all events that PIMSM main task receives, run the first one of the following two commands

debug ip pim-sm event

no debug ip pim-sm event

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

According to the output information, you can browse all events of current PIMSM.

Example

None

41.1.53 debug ip pim-sm hello

Syntax

To display the Hello packet received or transmitted by PIM-SM for debugging the neighbor's information, run the first one of the following two commands

debug ip pim-sm hello

no debug ip pim-sm hello

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

According to the output information, you can browse the Hello packets, including those received or transmitted by PIM-SM, to know what's going on the local machine or the neighbors

Results

The ports, source addresses and genid of the currently received or transmitted Hello packets can be displayed

Example

None

41.1.54 debug ip pim-sm jp

Syntax

To trace the Join/Prune event of (*, g) or (s, g), run the first one of the following two commands

debug ip pim-sm jp [packet | state- machine | A.B.C.D]

no debug ip pim-sm jp [packet | state- machine | A.B.C.D]

Parameter

Name	English prompt	Notes
state- machine	state-machine -- Trace state machine activity information	
packet	packet -- Trace information about packet	
A.B.C.D	A.B.C.D -- Group address for stm and packet output	

Default value

None

Command mode

EXEC

Usage guidelines

None

Example

None

41.1.55 debug ip pim-sm nbr

Syntax

To trace the related events of a neighbor, such as the addition of neighbor, aging deletion or DR selection, run the first one of the following two commands

debug ip pim-sm nbr

no debug ip pim-sm nbr

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

According to the output information of this command, you can browse neighbor change, neighbor refreshment, GENID change and DR selection

Example

None

41.1.56 debug ip pim-sm packet

Syntax

To trace the protocol control packets received or transmitted by PIM-SM, run the following command

debug ip pim-sm packet

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

After this command is run, the receiving/sending PIM-SM packet's type will be displayed

Example

None

41.1.57 debug ip pim-sm register

Syntax

To display the registration packet and register state event of PIM-SM, run the first one of the following two commands

debug ip pim-sm register [packet | state- machine | A.B.C.D]

no debug ip pim-sm register [packet | state- machine | A.B.C.D]

Parameter

Name	English prompt	Notes
state- machine	state-machine -- Trace state machine activity information	
packet	packet -- Trace information about packet	
A.B.C.D	A.B.C.D -- Group address for stm and packet output	

Default value

None

Command mode

EXEC

Usage guidelines

According to the output information, you can check the register event of PIM-SM

Example

None

41.1.58 debug ip pim-sm timer

Syntax

To display the change of all PIM-SM timers, including creation, deletion, stop and timeout, run the first one of the following two commands.

debug ip pim-sm timer

no debug ip pim-sm timer

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The PIM-SM timers include the Hello timer, the neighbor timeout timer, pim-sm route downstream timeout timer, pim-sm route entry timeout timer, the Join/Prune timer, the override timer, the prune pending timer, the keepalive timer, the assert timer, periodic query timer for unicast routing changes, the register timer, the register limit timer, management domain timer, BSM timer, BSM forwarding timer, the BSM timer, C-RP periodic notification timer, and C-RP trigger update timer, RP-SET keeps the timer and so on

Example

None

Chapter 42 ND Commands

42.1 debug ipv6 nd

Syntax

To enable the switch of printing ND debugging information, run the following command:

debug ipv6 nd [*entry* | *timer* | *X:X:X:X::X* | *adj-table*]

Parameter

Parameter	Description
entry	Stands for the switch of neighbor cache entry changes
timer	Stands for the switch of neighbor cache timer changes
X:X:X:X::X	Stands for the IPv6 address of neighbor cache
adj-table	Stands for the debug switch of neighbor adjacency table

Default

By default, the switch of printing ND debugging information is in disabled state

Command Mode

EXEC

Usage Guidelines

If the command carries with no extension parameters, all debugging switches are enabled

Example

None

Related Command

None

42.2 show ipv6 neighbors

Syntax

To display the current switch's neighbor cache, run the following command:

show ipv6 neighbors [interface | **summary**]

Parameter

Parameter	Description
interface	Display the IPv6 neighbor cache based on the interface
summary	Display summary IPv6 neighbor cache information

Default

Display all IPv6 neighbor cache information

Command Mode

EXEC

Usage Guidelines

None

Related Command

None

42.3 clear ipv6 neighbors

Syntax

To cancel on a switch all neighbor caches that are not configured manually, run the following command:

clear ipv6 neighbors

Parameter

None

Default

None

Command Mode

EXEC

Usage Guidelines

This command can only cancel all those neighbor caches automatically obtained by a switch itself, not those manually configured by the **ipv6 neighbor** command

Related Command

ipv6 neighbor

42.4 ipv6 neighbor

Syntax

To set neighbor caches of a switch, run the following command globally:

ipv6 neighbor *address6* **vlan** *vlanid mac*

Parameter

Parameter	Description
address6	Means the IPv6 address of the neighbor
vlanid	Stands for the ID of the VLAN port
mac	Means the link-layer address of a neighbor

Default

None

Command Mode

Global configuration mode

Usage Guidelines

You can use this command to set neighbor caches of a switch. These neighbor caches never times out and are always reachable until **no ipv6 neighbor** is run

Example

IPv6_config#ipv6 neighbor 1::1 vlan 1 00:e0::4c:5a:78:eb

The above-mentioned example shows how to set on port e1/1 a neighbor whose IPv6 address is 1::1 and whose link-layer address is 00:e0:4c:5a:78:eb

Related Command

show ipv6 neighbors

Chapter 43 Network Management Configuration Commands

43.1 snmp-server community

Syntax

To set the community access string of the accessible SNMP protocol, run **snmp-server community** in global configuration mode. To delete the specified community character string, use the no form of this command

snmp-server community [0|7] *string* [**view** *view-name*] [**ro | rw**] [*word*]

no snmp-server community *string*

no snmp-server community

Parameters

Parameters	Description
0	Sets the community string of the text
7	Sets the encrypted public string of the text
string	Means the community string of the accessible SNMP protocol, which is similar to the password
view view-name	(optional) stands for the previously defined view's name. In this view, the MIB objects, which are effective to the community, are defined
ro	(Optional) Designates the read-only permission. Those authorized workstations can only read the MIB objects
rw	(Optional) Designates the read-write permission. Those authorized workstations can read and modify the MIB objects
word	(optional) Specifies the name of IP ACL of the SNMP proxy, which can be accessed by the community string

Default

By default, the SNMP community string allows the read-only permission to all objects

Command Mode

Global configuration mode

Usage Guidelines

The following command shows how to delete a designated community

no snmp-server community *string*

The following command shows how to delete all communities

no snmp-server community

Example

The following example shows how to distribute the "comaccess" string to SNMP, allow the read-only access and designate IP ACL to use the community string

snmp-server community comaccess ro allowed

The following example shows how to distribute the "mgr" string to SNMP, allow to read and write the objects in the Restricted view

snmp-server community mgr view restricted rw

The following example shows how to delete the "comaccess" community

no snmp-server community comaccess

Related Command

access-list

snmp-server view

43.2 snmp-server contact

Syntax

To set the information about the contact person in a management node, run **snmp-server contact text** command in the global configuration mode. To delete the contact information, use the no form of this command

snmp-server contact *text*

no snmp-server contact

Parameters

Parameters	Description
text	Means the string of the information about the contact person

Default

The information about contact person is not set

Command Mode

Global configuration mode

Usage Guidelines

It corresponds to the sysContact of the MIB variable in the System group

Example

The following example shows the information about the contact person in a node

snmp-server contact Dial_System_Operator_at_beeper_#_27345

43.3 snmp-server engineID local

Syntax

To configure the SNMP engine ID of the local agent, run **snmp-server engineID local** command in the global configuration mode. To remove the SNMP engine ID of the local agent, use the no form of this command

snmp-server engineID local *engineID*

no snmp-serverr engineID local *engineID*

Parameters

Parameters	Description
engineID	SNMP engineID

Default

The SNMP engineID is not set

Command Mode

Global configuration mode

Usage Guidelines

The command is used to configure the SNMP engine ID of the local agent

Example

snmp-server engineID local 80000cf80300e00f3f56e3

43.4 snmp-server group

Syntax

To create or update a **snmp-server** group in global configuration mode, run the following first command; to

cancel this SNMP group, run the following second command. Format of the command is as follows:

snmp-server group [*groupname* { **v3 [auth | noauth | priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]

no snmp-server group *groupname*

Parameters

Parameters	Description
groupname	Stands for the name of the created or modified SNMP group
v3	Means the version ID of the SNMP protocol
auth|noauth|priv	Stands for the lowest security level of users in the SNMPv3 group
readview	Means the access permission of GET operations, which is defined by the view
writeview	Means the access permission of SET operations, which is defined by the view
notifyview	Stands for the access permission during the transmission of Trap packets, which is defined by the view
access-list	Allows users in the SNMP group to get through the IP access control list

Default

The readview allows all leaves of the Internet sub-tree to be accessed

Command mode

Global configuration mode

Usage Guidelines

The SNMP group is used to designate the access permission of the users in this group

Example

In the following example, an SNMP group is set and named as setter, the version ID of the SNMP protocol is 3, the security level is authentication and encryption, and the view that is accessed by the set operation is v-write

snmp-server group setter v3 priv write v-write

Related Command

snmp-server view

snmp-server user

43.5 snmp-server [host|hostv6]

Syntax

To specify the receiver of SNMP trap operation, run the first of the following commands in global configuration mode. To cancel this designated host, run the following second command

snmp-server host|hostv6 *host* **[udp-port** *port-num***] [permit|deny** *event-id***] {{version [v1 | v2c | v3]} | {[informs | traps] | [auth |noauth]}}** *community-string/user* **[authentication | configure| snmp]**

no snmp-server host *host community-string*

Parameters

Parameters	Description
host|hostv6	Sets the IPv4 or IPv6 trap host.
host	Means the host's name or the address of the Internet Uses bipv4 address in host Uses ipv6 address in hostv6
[udp-port *port-num***]**	(Optional) Specifies the ID of the UDP port, which transmits the traps
[permit|deny *event-id***]**	(Optional) Allows or blocks to transmit a designated event
{version [v1|v2c|v3]}	(Optional) Means the version ID of the SNMP protocol, which is used to transmit traps
[informs | traps]	(Optional) Specifies the type of trap for version V2C Informs: means the type of trap is "informs" Traps: means the type of trap is "traps"
[auth |noauth]	Specifies the trap authentication mode for version V3. **auth:** authentication **noauth:** non-authentication
community-string/user	Means a community string in version 1 and version 2c which is similar to the password and sent with the trap operations or means the username in version 3
[authentication | configure| snmp]	(optional) if no trap is designated, all generated traps will be sent to the host **authentication:** allows to transmit those authentication-error traps. **configure:** allows to transmit the SNMP-configure traps **snmp:** allows to transmit the SNMP traps

Default

This command is invalid in default settings. That is to say, no trap will be sent by default. If no command with any key word is entered, all traps with v1 standard are not sent by default

Command Mode

Global configuration mode

Usage Guidelines

If this command is not entered, the traps will not be sent. In order to enable a switch to send the SNMP traps. You must run **snmp-server host**. If the keyword "trap-type" is not contained in this command, all kinds of traps of this host will be activated. If the keyword "trap-type" is contained in this command, all trap types related with this keyword are activated. You can specify multiple trap types in this command for each host

If you designate multiple **snmp-server host** commands on the same host, the SNMP trap messages that are sent to the host will be decided by the community string and the trap type filtration in this command. (Only one trap type can be configured for a same host and a same community string)

The availability of the **trap-type** option depends on the OLT type and the attributes of routing software, which is supported by this OLT

Example

The following example shows how to transmit the RFC1157-defined SNMP traps to host 10.20.30.40. The community string is defined as comaccess

snmp-server host 10.20.30.40 comaccess snmp

The following example shows that the OLT uses the public community string to send all types of traps to host 10.20.30.40.

snmp-server host 10.20.30.40 public

The following example shows that only the authentication traps are effective and can be sent to host bob.

snmp-server host bob public authentication

Related Command

snmp-server queue-length

snmp-server trap-source

snmp-server trap-timeout

snmp-server event-id

snmp-server user

43.6 snmp-server location

Syntax

To set the location string of a node, run the first one of the following two commands in global configuration mode. To cancel this designated host, run the following second command

snmp-server location *text*

no snmp-server location

Parameters

Parameters	Description
text	The location string of a node is not set by default

Default

The location string of a node is not set by default

Command Mode

Global configuration mode

Usage Guidelines

It corresponds to the sysLocation of the MIB variable in the System group

Example

The following example shows how to define the actual location of a OLT

snmp-server location Building_3/Room_214

Related Command

snmp-server contact

43.7 snmp-server packetsize

Syntax

To define the maximum size of the SNMP packet when the SNMP server receives requests or responds, run the following first command in global configuration mode

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameters

Parameters	Description
byte-count	Stands for the integer bytes between 484 and 17940. The default value is 3000 bytes

Default

3000 bytes

Command Mode

Global configuration mode

Usage Guidelines

The command corresponds to the sysLocation of the MIB variable in the System group

Example

The following example shows how to set up a filter to filter those packets whose maximum length is 1024 bytes

snmp-server packetsize 1024

Related Command

snmp-server queue-length

43.8 snmp-server queue-length

Syntax

To set the queue length for each trap host, run the following first command in global configuration mode

snmp-server queue-length *length*

no snmp-server queue-length

Parameters

Parameters	Description
length	Stands for the number of trap events which can be saved in the queue (1-1000)

Default

10 trap events

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the queue length for each trap host. Once the trap messages are successfully transmitted, the switch will empty the queue

Example

The following example shows how to set up a message queue which can capture four events

snmp-server queue-length 4

Related Command

snmp-server packetsize

43.9 snmp-server trap-source

Syntax

To designate an interface to be the source address of all traps, run the following first command in global configuration mode. To cancel this interface, run the following second command

snmp-server trap-source *interface*

no snmp-server trap-source

Parameters

Parameters	Description
interface	Stands for the interface where SNMP traps generate. The parameters include the interface type and interface ID of the syntax mode of specific platform

Default

The interface is not designated

Command Mode

Global configuration mode

Usage Guidelines

When the SNMP server sends out a SNMP trap on whichever interface, the SNMP trap shall carry a trap address. If you want to use the trap address for tracking, you can use this command

Example

The following example shows how to designate interface vlan1 as the source address of all traps

snmp-server trap-source vlan1

Related Command

snmp-server queue-length

snmp-server host

43.10 snmp-server trap-timeout

Syntax

To set the timeout value of retransmitting traps, run the following first command in global configuration mode

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameters

Parameters	Description
seconds	Means an interval for retransmitting traps, whose unit is second (1-1000)

Default

30 seconds

Command Mode

Global configuration mode

Usage Guidelines

Before OLT software tries to send traps, it is used to look for the route of destination address. If no routes exists, traps will be saved in the retransmission queue. The **server trap-timeout** command decides the retransmission interval

Example

The following example shows how to set the retransmission interval to 20 seconds:

snmp-server trap-timeout 20

Related Command

snmp-server host

snmp-server queue-length

43.11 snmp-server user

Syntax

To create or update an**snmp-server user** in global configuration mode, run the following first command; to cancel this SNMP user, run the following second command. If the remote parameter is designated, a remote user will be configured; when a remote user is configured, the SNMP engine ID that corresponds to the IP address of this management station must exist. Format of the command is as follows:

snmp-server user *username groupname* **{ v3 [encrypted | auth] [md5 | sha]** *auth-password* **}**

no snmp-server user username groupname v3

Parameters

Parameters	Description
username	Stands for the name of the created or modified SNMP user
groupname	Stands for the group where the user is
v3	Stands for the SNMP version
[encrypted | auth]	Encryption type: Encrypted: packet encryption auth: packet authentication
{md5 | sha }	Means the method of encryption authentication
auth-password	Stands for the authentication password of the user. If this password is localized, it will be used as the authentication key and the encryption key of SNMPv3

Default

None

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the username and the password

Example

In the following example, an SNMP user is created, whose name is set-user and which belongs to setter, the version of the SNMP protocol is version 3, the security level is authentication and encryption, the password is 12345678, and MD5 is used as the harsh algorithm

snmp-server user set-user setter v3 encrypted auth md5 12345678

Related Command

snmp-server view

snmp-server group

43.12 snmp-server view

Syntax

To create or update a MIB view, run the first one of the following two commands in global configuration mode. To cancel a view in the SNMP server, run the second one of the following two commands

snmp-server view *view-name oid-tree* {**included | excluded**}

no snmp-server view *view-name*

Parameters

Parameters	Description
view-name	Updates or creates the label of a view
oid-tree	Means the object IDs of the ASN.1 sub-tree that must be contained or excepted from a view. The identifier sub-tree is used to designate a numeral-contained string, e.g., 1.3.6.2.4 or a system sub-tree. The sub-tree name can be found in all MIB trees. Means the view type. The parameter "included" or "excluded" must be specified
included | excluded	Means the view type. The parameter "included" or "excluded" must be specified

Default

None

Command Mode

Global configuration mode

Usage Guidelines

If other SNMP commands need a view as a parameter, you can use this command to create a view. By default, you need not define the view and you can see all the views, equivalent to Cisco-predefined everything views. The command is used to define the object the view sees

Example

The following example shows how to create the views of all objects in the MIB-II sub-tree

snmp-server view mib2 mib-2 included

The following example shows how to create the views of all objects, including those objects in the system group

snmp-server view phred system included

The following example shows how to create the views of all objects that includes the objects in the system groups but excludes the objects in system7(sysServices.7) and interface 1

snmp-server view agon system included

snmp-server view agon system.7 excluded

Related Command

snmp-server community

43.13 snmp-server source-addr

Syntax

To specify a source address for answering all SNMP requests, run the second one of the following two commands in global configuration mode. To cancel this interface, run the following second command

snmp-server source-addr *a.b.c.d*

no snmp-server source-addr

Parameters

Parameters	Description
a.b.c.d	Means the source address for all SNMP requests to be answered. Designate the source address of SNMP generating packets. The parameter is the IP address the device has set

Default

The default source address is the nearest routing address

Command Mode

Global configuration mode

Usage Guidelines

When the SNMP server transmits an SNMP request, you can run this command to designate a special source address

Example

The following example shows how to designate the IP address "1.2.3.4" of the designated interface as the source address of all SNMP packets

snmp-server source-addr 1.2.3.4

Related Command

None

43.14 snmp-server udp-port

Syntax

To specify the port number for the SNMP agent to receive packets, run the following first command in global configuration mode

snmp-server udp-port *portnum*

no snmp-server udp-port

Parameters

Parameters	Description
udp-port	Stands for the ID of the destination port to which SNMP traps are sent, which cannot be a command port ID. The value ranges from 1 to 65535

Default

It is the listening port of SNMP agent by default, that is, port 162

Command Mode

Global configuration mode

Usage Guidelines

The SNMP agent will listen to this port when SNMP server transmits SNMP packets

Example

The following example shows how to specify the listening port of SNMP agent to port 1234

snmp-server udp-port 1234

Related Command

None

43.15 snmp-server encryption

Syntax

To display the configured SNMP community, the SHA encryption password and the MD5 encryption password, run **snmp-server encryption** in global mode. This command is a once-for-all command, which cannot be saved or canceled by its negative form. Format of the command is as follows:

snmp-server encryption

Parameters

None

Default

The default settings is to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text

Command Mode

Global configuration mode

Usage Guidelines

This command is used to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text. In this way, the security of the password is guaranteed

Example

The following example shows how to show in the plain text the SNMP community, the SHA encryption password and the MD5 encryption password, which are set for host 90.0.0.3.

snmp-server encryption

Related Command

snmp-server community

snmp-server user

43.16 snmp-server trap-add-hostname

Syntax

To add the host name to the binding variable when SNMP sends traps, run the first one of the following two commands

snmp-server trap-add-hostname

no snmp-server trap-add-hostname

Parameters

None

Default

The hostname is not added to the binding variable list when traps are being transmitted

Command Mode

Global configuration mode

Usage Guidelines

This command is a great help in some cases when the NMS needs to locate which host sends these traps

Example

The following example shows how to enable the trap-to-hostname binding function

Router_config# snmp-server trap-add-hostname

43.17 snmp-server trap-logs

Syntax

To write the trap transmission records into logs, run the first one of the following

two commands

snmp-server trap-logs

no snmp-server trap-logs

Parameters

None

Default

The transmitted traps are not recorded by default

Command Mode

Global configuration mode

Usage Guidelines

After this function is enabled, the trap transmission records of a device can be sent to the log server and then you can know more about the running state of the device

Example

The following example shows how to the trap logs function

Router_config# snmp-server trap-logs

43.18 snmp-server set-snmp-dos-max

Syntax

To set the incorrect community login retry times in five minutes on the SNMP server, run the first one of the following two commands

snmp-server set-snmp-dos-max *retry times*

no snmp-server set-snmp-dos-max

Parameters

Parameter	Parameter Description
retry-times	Set the login times for a user to conduct the incorrect community login in five minutes

Default

The incorrect community login times is not limited

Command Mode

Global configuration mode

Usage Guidelines

This command can be used to prevent those SNMP host from guessing the device's community viciously, which lessening unnecessary CPU consumption of the device

Example

The following example shows how to enable the refuse service function and set the max trying times to 10 in five minutes

Router_config# snmp-server set-snmp-dos-max 10

43.19 snmp-server keep-alive

Syntax

To set the timely sending heartbeat trap, run **snmp-server keep-alive** in global configuration mode. The time interval is times

snmp-server keep-alive *times*

no snmp-server keep-alive

Parameters

Parameters	Description
times	The time interval of heartbeat trap

Default

The command is not configured by default

Command Mode

Global configuration mode

Usage Guidelines

The command must be used with snmp-server host

Example

The following example shows how to set the device sending heartbeat trap every 3 seconds

snmp-server keep-alive 3

Related Command

snmp-server host

snmp-server hostv6

43.20 snmp-server necode

Syntax

To set the information about the management node (the unique identifier of the device), run snmp-server necode text. To delete the identifier information, use the no form of this command

snmp-server necode *text*

no snmp-server necode

Parameters

Parameters	Description
text	Sets the information about the management node (the unique identifier of the device)

Default

The node identifier is not set

Command Mode

Global configuration mode

Usage Guidelines

The command is corresponding to the snmp private MIB variable

Example

The following example shows the information about the node

snmp-server necode Dial_System_Operator_at_beeper_#_27345

43.21 snmp-server event-id

Syntax

To create and set event list, run command snmp-server event-id in the global configuration mode. To delete the event list, use the no form of this command

snmp-server event-id *number* **trap-oid** *oid*

no snmp-server event-id *number* [**trap-oid** *oid*]

Parameters

Parameters	Description
number	The only identifier of event-id
oid	trap OID included in event-id

Default

The event list information is not set by default

Command Mode

Global configuration mode

Usage Guidelines

The command is used in host configuration

Example

The following example shows how to set trap whose trap OID is 1.2.3.4.5 to event ID 1

snmp-server event-id 1 trap-oid 1.2.3.4.5

43.22 snmp-server getbulk-timeout

Syntax

To set the timeout of processing getbulk request, run command snmp-server getbulk-timeout in the global configuration mode. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly. To delete the configuration, use the no form of this command

snmp-server getbulk-timeout *seconds*

no snmp-server getbulk-timeout

Parameters

Parameters	Description
seconds	The timeout of processing getbulk request

Default

The timeout of processing getbulk request is not set by default

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set the timeout of processing getbulk request. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly

Example

The following example shows how to set getbulk-timeout and set the timeout to 5 seconds

snmp-server getbulk-timeout 5

43.23 snmp-server getbulk-delay

Syntax

To set getbulk-delay time to prevent snmp occupying excessive cpu when snmp agent processing getbulk request, run command snmp-server getbulk-delay in the global configuration mode. The unit is 0.01 seconds. To delete the configuration, use the no form of this command

snmp-server getbulk-delay *ticks*

no snmp-server getbulk-delay

Parameters

Parameters	Description
ticks	Sets CPU interval time in processing getbulk request. The unit is 0.01s

Default

The command is not configured when CPU is processing getbulk request in full load

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set getbulk-delay time to prevent snmp from occupying excessive cpu when snmp agent processing getbulk request. The unit is 0.01s

Example

The following example shows how snmp agent pauses one ticks when getting one result in configuring getbulk

snmp-server getbulk-delay 1

43.24 show snmp

Syntax

To monitor SNMP input and output statistics, including illegal community character strings, the number of errors and request variables, run command **show snmp**. To show SNMP engine information, run command **show snmp engineID**. To show SNMP trap host information, run commmand **show snmp host**. To show SNMP view information, run command **show snmp view**. To show snmp mibs registration information, run command **show snmp mibs**. To show snmp group information, run command **show snmp group**. To show SNMP user information, run command show **snmp user**

show snmp [engineID |host | view | mibs |group|user]

Parameters

Parameters	Description
engineID	Shows SNMP engine information
host	Shows SNMP trap host information
View	Shows SNMP view information
mibs	Shows SNMP MIB registration information
group	Shows SNMP group information
user	Shows SNMP user information

Default

None

Command Mode

EXEC mode or global configuration mode

Usage Guidelines

The command **show snmp** is used to show SNMP input and output statistics

The command **show snmp engineID** is used to show SNMP engine information

The command **show snmp host** is used to show SNMP trap host information

The command **show snmp view** is used to show SNMP view information

The command **show snmp mibs** is used to show mib registration information

The command **show snmp group** is used to show SNMP group information

The command **show snmp user** is used to show SNMP user information

Example

The following example shows how to list SNMP input and output statistics

#show snmp

37 SNMP packets input

0 Bad SNMP version errors

4 Unknown community name

0 Illegal operation for community name supplied

0 Snmp encoding errors

24 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

28 Get-next PDUs

0 Set-request PDUs

78 SNMP packets output

0 Too big errors (Maximum packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

24 Get-response PDUs PDUs

13 SNMP trap PDUs

Meaning of statistics information of SNMP Agent receiving and sending packets:

Displayed Information	Meaning
Unknown community name	Unknown community name
Illegal operation for community name supplied	Illegal operation
Encoding errors	Encoding errors
Get-request PDUs	Get-request PDUs
Get-next PDUs	Get-next PDUs
Set-request PDUs	Set-request PDUs
Too big errors	The packets are too big to generate response packets
No such name errors	No such name errors
Bad values errors	Bad values errors

General errors	General errors
Get-response PDUs	Get-response PDUs
Trap PDUs	SNMP trap packets

The following example shows how to show SNMP trap host information

#show snmp host

Notification host: 192.2.2.1 udp-port: 162 type: trap

user: public security model: v1

The following example shows how to show SNMP view information.

#show snmp view

mib2 mib-2 - included permanent active

Related Command

snmp-server host

snmp-server view

43.25 debug snmp

Syntax

To show SNMP event, packet sending and receiving process and error information, run command **debug snmp**

debug snmp [*error* | *event* | *packet*]

To stop showing the information, run command **no debug snmp**

no debug snmp

Parameters

Parameters	Description
error	Enable the debug switch of SNMP error information
event	Enable the debug switch of SNMP event information
packet	Enable the debug switch of SNMP input/output packets

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable SNMP debug information switch and output SNMP event, information of sending and receiving packets, which is helpful for SNMP fault diagnosis

Example

The following example shows how to debug SNMP receiving and sending packets

switch#debug snmp packet

Received 49 bytes from 192.168.0.29:1433

0000: 30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0 0..-.....public.

0016: 82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00 .....}.....0..

0032: 10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 .0.....+.....

0048: 00 .

Sending 52 bytes to 192.168.0.29:1433

0000: 30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2 0..0.....public.

0016: 82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00 ..!..}.....0..

0032: 13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43 .0.....+.....C

0048: 03 00 F4 36 ...6

Received 51 bytes from 1192.168.0.29:1434

0000: 30 82 00 2F 02 01 00 04 06 70 75 62 6C 69 63 A0 0../.....public.

0016: 82 00 20 02 02 6B 84 02 01 00 02 01 00 30 82 00 .. ..k.....0..

0032: 12 30 82 00 0E 06 0A 2B 06 01 02 01 02 02 01 02 .0.....+.....

0048: 01 05 00 ...

Sending 62 bytes to 192.168.0.29:1434

0000: 30 82 00 3A 02 01 00 04 06 70 75 62 6C 69 63 A2 0..:.....public.

0016: 82 00 2B 02 02 6B 84 02 01 00 02 01 00 30 82 00 ..+..k.....0..

0032: 1D 30 82 00 19 06 0A 2B 06 01 02 01 02 02 01 02 .0.....+.....

0048: 01 04 0B 45 74 68 65 72 6E 65 74 30 2F 31 ...Ethernet0/1

Domain	Description
Received	Stands for SNMP receiving packets
192.168.0.29	Stands for source IP address
1433	Stands for source address port number
51 bytes	Stands for the length of receiving packets
30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0 82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00 10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 00	Stands for packets after SNMP ASN encoding
0..-.....public. .....}.....0.. .0.....+..... .	Stands for ASCII character of receiving packets. "." means not in the range of ASCII character
sending	SNMP sending packets
192.168.0.99	Stands for the destination IP address
1433	Stands for the source address port number
52 bytes	Stands for the length of sending and receiving packets
30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2 82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00 13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43 03 00 F4 36	Stands for packets after SNMP ASN encoding
0..0.....public. ..!..}.....0.. .0.....+.....C ...6	Stands for ASCII character of sending and receiving packets. "." means not in the range of ASCII character

The following example shows how to debug SNMP events

switch#debug snmp event

Received SNMP packet(s) from 192.2.2.51

SNMP: GETNEXT request

-- ip.ipReasmFails.0

SNMP: Response

>> ip.ipFragOKs.0 = 1

Received SNMP packet(s) from 192.2.2.51

SNMP: GETNEXT request

-- ip.ipFragOKs.0

SNMP: Response

>> ip.ipFragFails.0 = 0

Received SNMP packet(s) from 192.2.2.51

SNMP: GETNEXT request

-- ip.ipFragFails.0

SNMP: Response

>> ip.ipFragCreates.0 = 2

Domain	Description
SNMP	Stands for the current debug SNMP protocol
GETNEXT request	SNMP getnext request
RESPONSE	SNMP response
--	Stands for receiving packets
>>	Transmitting packets
ip.ipReasmFails.0	Stands for MIB OID of access request
ip.ipFragOKs.0 = 1	Stands for being accessed MIB OID and the return value

43.26 rmon alarm

Syntax

rmon alarm *index variable interval* {absolute | delta} rising-threshold *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [repeat] [owner *string*]

To configure a rmon alarm entry, run the above command

Parameters

Parameters	Description
index	Stands for the index of the event table Value range: 1-65535
variable	Stands for the object needs to be monitored. Value range: oid of the monitored object
interval	Stands for the sampling interval Value range: 1~ 2147483647
value	Stands for the alarm threshold Value range: -2147483648~ 2147483647
eventnumber	Stands for the event index generated after reaching the threshold. Value range: 1~65535
repeat	Stands for the repeat trigger event
string	Stands for the owner description information Value range: the length of the character string is 1~31

Default

eventnumber is not set by default

repeat is not set by default

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to monitor the value of specified object. The certain event will be triggered when the value exceeds the threshold

Example

The following example shows how to set an alarm entry to monitor the object ifInOctets.2 and the sampling interval is 10. When the sampling interval increases more than15, the event 1 will be triggered. When the sampling interval decreases more than 25, the event 2 will be triggered

rmon alarm 1 1.3.6.1.2.1.2.2.1.10.2 10 absolute rising-threshold 15 1 falling-threshold 25 2 repeat owner switch

43.27 rmon event

Syntax

rmon event *index* [description *des-string*] [log] [owner *owner-string*] [trap *community*] [ifctrl *interface*]

To configure a rmon event entry, run the above command

no rmon event index

To delete a rmon event entry, run the above command

Parameters

Parameters	Description
index	Stands for the index of the event table Value range: 1-65535
des-string	Stands for the event description character string. Value range: 1~127
owner-string	Stands for the owner character string. Value range: 1~31
community	Stands for the community name when generating trap. Value range: 1~31
interface	Stands for the shutdown port that the event controls

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to set a rmon event entry. It is used for alarm

Example

The following example shows to set one rmon event entry to 6 and the description character string to example; add one item in the log entry when triggering the event and generates trap with public as the community name

rmon event 6 log trap public description example owner switch

43.28 rmon collection stats

Syntax

rmon collection stats *index* [*owner string*]

To set rmon statistics function, run the above command

no rmon collection stats ***index***

To delete rmon stats, run the above command

Parameters

Parameters	Description
index	Stands for the index of the statistics entry. Value range: 1~65535

string	Stands for the owner character string. Value range: the length of the character string is 1~31

Default

None

Command Mode

Interface configuration mode

Usage Guidelines

The command must be configured in the interface mode

Example

The following example shows how to enable the statistics function on gigabit Ethernet interface g0/1

int g0/1

rmon collection stats 2 owner switch

43.29 rmon collection history

Syntax

rmon collection history *index* [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]

To configure a history control entry, run the above command

no rmon collection history ***index***

To delete a history index, run the above command

Parameters

Parameters	Description
index	index Value range: 1-65535
bucket-number	The entry of all history record control entries nearest to the bucket-number need to be reserved. Value range: 1~65535
second	Stands for the time interval. Value range: 1~3600
owner-name	Stands for the owner character string. Value range: the length of the character string is 1~31

Default

The default bucket-number is 50 and the default second is 1800

Command Mode

Interface configuration mode

Usage Guidelines

The command is used to configure in the interface mode. It is used for adding one entry to the history control table

Example

The following example shows how to add the history control entry on the gigabit Ethernet interface g0/1 and save the statistics of latest 20 time intervals.(Each time interval is 10 seconds.)

int g0/1

rmon collection history 2 buckets 20 interval 10 owner switch

43.30 show rmon

Syntax

show rmon [alarm] [event] [statistics] [history]

To show rmon configuration, run the above command

Parameters

None

Default

None

Command Mode

Other modes except the user mode

Usage Guidelines

To show rmon configuration, run the above command

Example

To show rmon configuration, run the above command

show rmon

Chapter 44 IP Address Configuration Commands

44.1 Arp static

Syntax

To configure static ARP mapping, run the following command. The static ARP mapping will will not be deleted from the arp table when the interface vlan exists. To delete the configured static ARP mapping, use the no arp static command

arp static *ip-address hardware-address vlan*

no arp static *ip-address vlan*

Parameter

Parameter	Description
ip-address	IP address corresponding to the local data-link address
hardware-address	Physical address of local data-link address
vlan	vlan belongs to the static arp

Default

No entries are permanently installed in the ARP cache

Command Mode

Global configuration mode

Usage Guidelines

The common host all supports dynamic ARP analysis, so user doesn't need to configure static ARP entries for host

In general, run **no arp staticip_address vlan** to delete static arp. If the interface vlan port to which a static arp belongs is deleted, the static arp will also be deleted

Example

The following example shows how to configure a static arp with the IP address of 1.1.1.1 and the host's MAC address of 00:12:34:56:78:90 under vlan1

arp static 1.1.1.1 00:12:34:56:78:90 vlan1

Related Commands

clear arp

44.2 arp timeout scan_intervel

Syntax

To configure the interval for active re-probing of the ARP cache, use the **arp timeout scan_intervel minutes**. To restore the default value, use the no form of this command

arp timeout scan_intervel minutes

no arp timeout scan_intervel

Parameter

Parameter	Description
minutes	Configures the interval (minutes) for the active re-probing of the ARP cache. <1-255>

Default

1 minute

Mode

Global configuration

Usage Guidelines

Dynamic arp has an aging time. After the aging time expires, the arp will be deleted. After re-detecting the arp, if it is learned, the time can be reset

Example

The following example shows how to set the ARP active reprobing interval to 2 minutes

arp timeout scan_intervel 2

Related Commands

arp timeout stale_threshold

arp timeout pending_timeout

44.3 arp timeout stale_threshold

Syntax

To configure the aging detection time of dynamic arp, use the following command. To restore the default seeting, use the no form of this command

arp timeout stale_threshold *minutes*

no arp timeout stale_threshold

Parameter

Parameter	Description
minutes	Configures the aging detection time of dynamic arp (minutes) <1-255>

Default

4 times of arp timeout scan_intervel

Command Mode

Global configuration mode

Usage Guidelines

Run the command to set the dynamic arp aging time, and thesetting will be deleted if the arp update is not received during this period. The default time is four times the detection time, and it is modified with the change of the detection time configuration, unless it has its own configuration

Example

The following example shows how to set the dynamic arp deletion time to 10 minutes

arp timeout stale_threshold 10

Related Commands

arp timeout scan_intervel

44.4 arp timeout pending_timeout

Syntax

To configure the deletion time of incomplete arps, run the following command

arp timeout pending_timeout minutes

no arp timeout pending_timeout

Parameters

Parameter	Description
minutes	Configures the deletion time of incomplete arps (minutes) <1-255>

Default Value

2 times of arp timeout scan_intervel

Command Mode

Global configuration mode

Usage Guidelines

The first ARP cache resolution will generate an incomplete entry and this command will then be used to set the life-time of this incomplete entry

Incomplete arp deletion time and other dynamic arp deletion time are separated, the default is twice the detection time. The the deletion time of incomplete arps is modified with the detection time configuration change, unless it has its own configuration

Example

The following example shows how to the deletion time of incomplete arps to 3 minutes

arp timeout pending_timeout 3

Related Command

arp timeout scan_intervel

arp timeout stale_threshold

44.5 arp timeout dynamic_arp_mac_check_enable

Syntax

To configure whether to enable mac detection for dynamic arp, run the following command. To return to the default setting, use the no form of this command

arp timeout dynamic_arp_mac_check_enable

no arp timeout dynamic_arp_mac_check_enable

Parameters

None

Command Mode

Global configuration mode

Usage Guidelines

By default, only mac detection is performed for static arp. The physical egress of static arp is updated according to the mac table egress. Whether dynamic arp is enabled for detection needs to be configured, because the detection is long-term polling and occupies a certain amount of cpu resources

Example

The following example shows how to enable the mac detection of the dynamic arp :

arp timeout dynamic_arp_mac_check_enable

Related Command

arp timeout mac_check_interval

44.6 arp timeout mac_check_interval

Syntax

To configure the interval for mac checking of arp, run the first one of the following commands. To return to the default setting, use the no form of this command

arp timeout mac_check_interval *seconds*

no arp timeout mac_check_interval

Parameter

Parameter	Description
seconds	the interval for mac checking of arp (s) <1-255>

Default

3s

Command Mode

Global configuration mode

Example

The following example shows how to configure the mac check time of arp to 2 seconds

arp timeout mac_check_intervel 2

Related Commands

arp timeout dynamic_arp_mac_check_enable

44.7 clear arp

Syntax

To clear all dynamic entries from the ARP cache, use the following command

clear arp [ip-address [mask | vlan vlanid]]

Parameter

Parameter	Description
ip-address	IP or subnets
mask	Subnets mask

vlanid	Vlan number

Command Mode

EXEC

Example

The following example removes all dynamic entries from the ARP cache:

clear arp

Related Command

arp static

44.8 ip address

Syntax

To set an IP address and mask for an interface, use the **ip address** command. Currently, there is no strict regulation to distinguish A.B.C IP address. But multicast address and broadcast address can not be used (all host section is '1'). Other than the Ethernet, multiple interfaces of other types can be connected to the same network. Other than the unnumbered interface, the configured network range to the Ethernet interface can not be the same as the arbitrary interfaces of other types. Generally, one primary address and unlimited number of secondary addresses can be configured on an interface. The secondary address can only be configured after the primary address is configured, and the primary address can only be deleted after all the secondary addresses are deleted. IP packets generanted by the system, if the upper application does not specify the soruce address, the switch will use the IP address configured on the sending interface that on the same network range with the gateway as the source address of the packet. If the IP address is uncertain (like interface route), the switch will use the primary address of the sending interface. If the ip address is not configured on an interface, also it is not the unnumbered interface, and then this interface will not deal with any IP packet

To remove an IP address or disable IP processing on an interface, use the no ip address command to clear one or all IP addresses on the interface

ip address *ip-address mask* [secondary]

no ip address *ip-address mask*

no ip address

Parameter

Parameter	Description
ip-address	IP address
mask	IP mask
secondary	(Optional) Indicates the configured IP slave address, if not specified, the IP primary address is configured

Default

No IP address is defined for the interface

Command Mode

interface configuration mode

Usage Guidelines

If the switch is configured with a secondary IP address on a certain physical network segment, other systems on the same physical network segment must also be configured with secondary IP addresses on the same logical network segment, otherwise routing loops will easily occur

When using the OSPF protocol, make sure that the secondary address on an interface is in the same OSPF area as its primary address

Example

In the following example, 202.0.0.1 is the primary address and 255.255.255 is the mask for interface VLAN 10. In addition, two secondary IP addresses 203.0.0.1 and 204.0.0.1 are configured:

interface vlan 10

ip address 202.0.0.1 255.255.255.0

ip address 203.0.0.1 255.255.255.0 secondary

ip address 204.0.0.1 255.255.255.0 secondary

44.9 show arp

Syntax

To display the entries in the Address Resolution Protocol (ARP) table, including the ARP mapping of interface IP address, the static ARP mapping that user configures and the dynamic ARP mapping, use the **show arp** command.

show arp

Parameter

This command has no parameters or keywords

Mode

EXEC

Usage Guidelines

The display includes:

Parameter	Description

Time	Living time, update the ARP entry to the present, unit: minute
IP4	Displays the network address that maps with the physical address. IP address, for example
Flags	Arp type, S means static arp, D means dynamic arp, and F means not to join the fib table
Status	Arp Status. I means incomplete arp, G means next hop as GATEWAY, D means protocol down state, and C means ready to delete
Ethernet	Displays the physical address that corresponds to the network address. It is empty for the unanalyzed entries
Others	Ref respectively indicates the number of routing entries and cache entries issued by this arp as the egress, and realstate is the actual state flag of some arps

Example

The following command displays ARP cache

switch#show arp

Arp total num:1

Time	IP4	Flags	Status	Ethernet	Interface
0	1.1.1.1	S	I	12:34:56:78:90:00	vlan1230 phy0 ref=0,0 realstate=1

44.10 show arp statistics

Syntax

To show ARP related statistical table items, use the following command

show arp statistic

Command Mode

EXEC

Usage Guidelines

Display description:

Total statistics	Including total number of arp, incomplete arp, complete arp
Cache statistics	Total number of cache statistics
Statistics of the hardware table entries	The statistics of the hardware table entries are distributed, including the statistics of the number of entries issued and the number of returned entries

Example

The following command displays ARP statistics:

switch_config#show arp statistics

Total ARP:1

Complete ARP:0, Incomplete ARP:1

Total cache:0

HWRT operate wait:29

HWRT operate over:29

44.11 show arp timeout

Syntax

To show configuration information related to ARP aging detection, use the following command

show arp timeout

Command Mode

EXEC

Usage Guidelines

The displayed information includes:

current time	Time record after boot
Full scan interval	Re-delivery interval (minutes).
Stale purge threshold	The delete time that not updated by Arp
Incomplete timeout	Delete time for incomplete arp
Mac check on dynamic arp	Whether to perform mac detection on dynamic arp
Mac check interval	Mac detection interval

Example

The following command displays the ARP aging detection configuration information:

Switch(config)#show arp timeout

IP neighbor scan enabled for IPV4 neighbors - current time is 1112893.0822 sec

Full scan interval: 1 min

Stale purge threshold: 4 min

Incomplete timeout:2 min

Mac check on dynamic arp:Enable

Mac check interval: 3 sec

44.12 show ip interface

Syntax

To display the IP configuration on interface, use the **show ip interface** command

show ip interface [**type** *number* | ***brief***]

Parameter

Parameter	Description
type	(Optional) port type
number	(Optional) port number
brief	(Optional) Displays the brief of ip protocols of all vlan ports

Command Mode

EXEC

Usage Guidelines

If the interface link layer is usable, the line protocol is marked "Protocol up." If you configure IP address on this interface, the switch will add a direct route to the routing table. If the link layer protocol is marked “Protocol down”, the direct route will be deleted. This command displays the specified interface information if specified interface type and number, or IP configuration information of all interfaces will be displayed

Example

The following example shows how to display IP configuration on port vlan 10

switch#show ip interface vlan 10

44.13 show ip cache

Syntax

To display all forwarding cache entries which are the entries after the hardware entries are issued, use the following command

show ip cache

clear arp

Parameter

None

Command Mode

EXEC

Usage Guidelines

The IP cache will be cleared when the egress arp is deleted

The displayed information includes:

Cache total num	Total ip cache quantity
number	Serial number
Dst ip	Address, a network address mapped to a physical address, such as an IP address

Example

The following example shows how to display the ip cache

switch#show ip cache

Related commands

clear arp

Chapter 45 NTP Configuration Commands

45.1 ntp master

Syntax

ntp master primary command is used to set the device as the original NTP server (stratum=1)

ntp master secondary command is used to set device as the secondary NTP server

no ntp master command is used to disable NTP server

Parameter

None

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

If the device is not configured with NTP server (**ntp server** command is not configured), **ntp master primary** command must be configured. Or the switch cannot provide time synchronization service. **ntp master secondary** command must be run when the switch configures NTP server. Moreover, the switch can provide time synchronization service to the NTP client in condition its own time synchronization is realized.

Example

Switch_config#ntp master primary

Switch_config#ntp master secondary

Switch_config#no ntp master

Related Command

ntp server

ntp peer

45.2 ntp client

Syntax

ntp client enable

no ntp client enable

To enable NTP client time synchronization function, run the above command. To disable NTP client time synchronization function, use the no form of this command

Parameter

None

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

When the device needs to synchronize time with the remote clock, it needs to perform **ntp client enable** after configuring the ntp server, otherwise synchronization will not proceed

Example

Switch_config#ntp client enable

Switch_config#no ntp client enable

Related Commands

ntp server

ntp peer

45.3 ntp authentication enable

Syntax

ntp authentication enable command

no ntp authentication enable

To enable NTP identity authentication, run the above command. To return to the default setting, use the no form of this command

Parameter

None

Default

Disabled

Command Mode

Global Configuration Mode

Usage Guidelines

For a secure network, NTP identity authentication must be enabled when operating NTP protocol. The identity authentication ensures that the client only realize time synchronization with the server which passes the identity authentication. Thus, the client will not obtain error time information from the illegal server

Example

Switch_config#ntp authentication enable

Related Commands

ntp authentication key

ntp authentication trusted-key

45.4 ntp authentication key

Syntax

ntp authentication key *keyid* **md5** *password*

no ntp authentication key *keyid*

To set NTP identity authentication key, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
keyid	The serial number of the authentication key. The value ranges from 1 to 4294967295
password	The key of keyed. The length ranges from 1 to 50

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to set identity authentication key. The client and the server must set the same key serial number and key value, or they cannot realize time synchronization

After set NTP authentication key, Set the key as the trusted key by command **ntp authentication trusted-key**. The trusted key will automatically disappear from the trusted key list when it is deleted.There is no need to run command "**no ntp authentication trusted-key**"

The command can set multiple ntp authentication key commands

Example

Switch_config#ntp authentication key 5 md5 abc123

Switch_config#no ntp authentication key 5

Related Commands

ntp authentication enable

ntp authentication trusted-key

45.5 ntp authentication trusted-key

Syntax

ntp authentication trusted-key *keyid*

no ntp authentication trusted-key *keyid*

To set the created key as the trusted key, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
keyid	The serial number of the trusted key. The value ranges from 1 to 4294967295

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enable the identity authentication function, the client can only time synchronize with the server providing the trusted key. If the key provided by the server is not trusted, the client cannot synchronize to the NTP server

The command must be configured after the key is set. The trusted key will automatically disappear from the trusted key list when it is deleted. There is no need to run command "**no ntp authentication trusted-key**"

Example

Switch_config#ntp authentication trusted-key 5

Switch_config#no ntp authentication trusted-key 5

Related Commands

ntp authentication enable

ntp authentication key

45.6 ntp server

Syntax

ntp server *ip-address* [**version** *number* | **key** *keyid* | **vrf** *vrf-name*]*

no ntp server *ip-address*

To set NTP server, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
ip-address	NTP Server IP address
number	NTP version number, the value ranges from: <1-4>, the default value is 4
keyid	When sending NTP packets to the NTP server, calculate the packet information abstract with the key corresponds to the keyid. The value ranges from 1 to 4294967295. If the parameter is not set, the device will not authenticate the identity of the server, or vice verse
vrf-name	Specifies the VPN routing and forwarding instance to which it belongs

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

After setting the NTP server, the device can time synchronize with the server, but the time of the server will not synchronize to the device

The command can be used to set multiple ntp server commands. If the NTP server in the public network is applied, at least 4 different NTP servers need to be configured (in order to exclude the wrong clock source)

Example

Switch_config#ntp server 1.1.1.1 version 4 key 5

Related Commands

ntp authentication enable

ntp authentication key

ntp authentication trusted-key

45.7 ntp peer

Syntax

ntp peer *ip-address* [**version** *number* | **key** *keyid* | **vrf** *vrf-name*]*

no ntp peer *ip-address*

To designate the NTP peer for the device, run the first one of the above commands. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
ip-address	NTP peer IP address
number	NTP version number. The value ranges from 1 to 4. The default value is 4
keyid	When sending NTP packets to the NTP server, calculate the packet information abstract with the key corresponds to the keyid. The value ranges from 1 to 4294967295. If the parameter is not set, the device will not authenticate the identity of the server, or vice verse
vrf-name	Specifies the VPN routing and forwarding instance to which it belongs

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Designate the NTP peer and the device can time synchronize with the peer in condition that it has synchronized. The command is usually used for mutual backup of the NTP server, not applicable for the client. To designate the NTP server, run the command **ntp server**.

Example

Switch_config#ntp peer 1.1.1.2 version 3 key 5

Related Commands

ntp authentication enable

ntp authentication key

ntp authentication trusted-key

45.8 show ntp

Syntax

show ntp [**status**]

To show NTP current status, run the above command

show ntp associations [**detail**]

To show NTP association status, run the above command

show ntp timers

To show NTP timer status, run the above command

Parameter

None

Default

None

Command Mode

EXEC

Usage Guidelines

Show NTP relevant information

Example

Switch#show ntp

Time-zone: GMT+8:00, Shanghai

Current time: 2014-05-21 10:45:26

Clock Status: synchronized

Clock Stratum: 3

Leap Indicator: 0

Reference ID: 211.233.84.186

Clock Jitter: 0.004149

Clock Precision: -18

Clock Offset: 6.561 ms

Root Delay: 172.153 ms

Root Dispersion: 587.873 ms

Query Interval: 0 s

Packets Sent: 30788

Packets Received: 27969 (bad version: 0)

Reference Time: 2014-05-21 10:41:37

Last Update Time: 2014-05-21 10:37:08

Switch#show ntp associations

ip address	reference clock	st	poll	reach	delay	offset	dispersion
61.110.197.50	204.123.2.5	2	64	377	59.99	0.96	2.7
27.114.150.12	193.190.230.65	2	64	377	489.97	-34.56	3.1
*211.233.84.186	204.123.2.5	2	64	377	19.99	9.15	3.0
198.55.111.50	216.229.0.50	3	64	377	229.98	-40.09	3.4
199.241.31.224	132.163.4.103	2	64	377	198.04	2.51	3.6
204.2.134.163	241.199.164.101	2	64	360	169.97	-17.16	942.8

Note: * system peer(master), poll(s), delay(ms), offset(ms), dispersion(ms)

Total Associations: 6

Related Command

None

45.9 debug ntp

Syntax

debug ntp packet

To enable NTP packet debug switch, run the above command

debug ntp event

To enable NTP event debug switch, run the above command

debug ntp error

To enable NTP error debug switch, run the above command

debug ntp all

To enable NTP all debug switches, run the above command

no debug ntp

To disable all debug switches, run the above command

Parameter

None

Default

None

Command Mode

EXEC

Usage Guidelines

Check NTP running process by debug information

Example

None

Related Command

None

45.10 time-zone

Syntax

time-zone *name offset-hour* [*offset-minute*]

no time-zone

To enable time zone function, run the first one of the above commands

To return to the default setting, use the no form of this command

Parameter

Parameter	Description
name	Name of the time zone
offset-hour	Hour off-set of local time to UTC time (-12~12)
offset-minute	Minute offset of local time to UTC time (0~59); the default value is 0

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to transfer UTC to the local time

Example

Switch_config#time-zone Beijing 8

Related Command

None

45.11 summer-time

Syntax

summer-time *name* absolute|periodical date|week start *start-time* end *end-time* [*offset*]

no summer-time

To set and enable the summer time, run the first one of the above commands

To disable the summer time, use the no form of this command

Parameter

Parameter	Description
name	Name of the summer time
absolute|periodical	Is daylight saving time repeated? 'absolute' represents that the summer time is only executed once, 'perriodical' represents that the summer time is effective every year
date|week	Date format, date represents the start and end date of summer time as specific year, month, and day, while week represents the start and end date of summer time as set to the x-th week of month x
start-time	Start date of summer time
end-time	End date of summer time
offset	The offset time of summer time (in minutes), defaults to 60 minutes

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Using this command will enable or disable the summer time

Example

The following example shows how to configure periodical summer time from 0:00 on the first Monday of July to 23:00 on the first Sunday of August:

Switch_config#summer-time Shanghai periodical week start 00:00 7 first Monday end 23:00 8 first Sunday

The following example shows how to configure absolute summer time from 00:00 on July 3, 2023 to 00:00 on August 3, 2023

Switch_config#summer-time Shanghai absolute date start 00:00 2023 7 3 end 00:00 2023 8 3

Related Command

None

Chapter 46 OAM Configuration Commands

46.1 ethernet oam

Syntax

[**no**] **ethernet oam**

To enable or disable the OAM function, run [**no**] **ethernet oam**

Parameter

None

Default

Ethernet OAM is disabled by default

Command Mode

Port configuration mode

Usage Guidelines

None

Example

The following commands are used to enable the OAM function on GigaEthernet 0/2 interface

Switch#

Switch#config

Switch_config#interface g0/2

Switch_config_g0/2#ethernet oam

46.2 ethernet oam {max-rate | min-rate | mode | timeout }

Syntax

[**no**] **ethernet oam {max-rate** *value1* **| min-rate** *value2* **| mode {active | passive} | timeout** *value3***}**

ethernet oam max-rate ***value1*** is used to set the fastest transmission rate of the OAM packet

ethernet oam max-rate ***value2*** is used to set the slowest transmission rate of the OAM packet

ethernet oam mode {active | passive} is used to set the OAM mode

ethernet oam timeout ***value3*** is used to set the timeout time of the OAM connection

Parameter

Parameter	Description

value1	Fastest transmission rate, which ranges between 1 and 10. Its unit is packet/second
value2	Slowest transmission rate, which ranges between 1 and 10. Its unit is second
value3	Timeout time of the OAM connection, which ranges between 2 and 30 and whose unit is second

Default

The value of **max-rate** is 10

The value of **min-rate** is 1

The value of **timeout** is 5

The value of **mode** is **active**

Command Mode

Port configuration mode

Usage Guidelines

This command can be used to configure some optional parameters for establishing the OAM connection

Example

The following example shows how to set the fastest and slowest connection rates of the OAM on the GigaEthernet 0/2 interface to 5 packets/second, the connection timeout time to 10 seconds and the OAM mode to **passive**

Switch #config

Switch_config#

Switch_config#interface g0/2

Switch_config_g0/2# ethernet oam max-rate 5

Switch_config_g0/2#ethernet oam min-rate 5

Switch_config_g0/2#ethernet oam timeout 10

Switch_config_g0/2#ethernet oam mode passive

46.3 ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action

Syntax

ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action error-disable-interface

no ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action

This command is used to configure the trigger action after the remote fault instruction is received

Parameter

None

Default

No trigger action is conducted after the remote fault instruction is received

Command Mode

Port configuration mode

Usage Guidelines

BDCOM switch cannot generate the LINK FAULT packets and the Critical Event packets. However, these packets will be handled if they are received from the remote terminal. BDCOM switch can transmit and receive the Dying Gasp packet. When the local port enters the **errdisabled** state or is closed by the administrator or the OAM function of the local port is closed by the manager, the Dying Gasp packet will be transmitted to the remote terminal that connects the local port

Example

The following example shows how to enable action error-disable-interface after receiving remote link fault instruction in the GigaEthernet0/1:

Switch_config#interface g0/1

Switch_config_g0/1#ethernet oam remote-failure link-fault action error-disable-interface

46.4 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high

Syntax

[**no**] **ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high {none |** *value***}**

To configure the high threshold for link monitoring, run the previous command

Parameter

Parameter	Description
Value	Error-signal period event ranges between 1 and 65535, whose unit is signal number
	Error-frame event ranges between 1 and 65535, whose unit is frame number
	Error-frame event ranges between 1 and 65535, whose unit is frame number
	Error-frame second event ranges between 1 and 900, whose unit is second
	Error-CRC event ranges between 1 and 65535, whose unit is frame number

Default

The default value of each general link event is **none**

Command Mode

Port configuration mode

Usage Guidelines

After the high threshold of an event and **ethernet oam link-monitor high-threshold action error-disable-interface** are configured, the local port enters the **errdisabled** state when the local port receives the high threshold of the event

Example

The following example shows how to configure the high threshold of the error-frame event to 10 on interface GigaEthernet0/2

Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold high 10

46.5 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low

Syntax

[**no**] **ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low {none |** *value***}**

To configure the low threshold for link monitoring, run the previous command

Parameter

Parameter	Description
Value	Error-signal period events ranges between 1 and 65535, whose unit is signal number
	Error-frame event ranges between 1 and 65535, whose unit is frame number
	Error-frame event ranges between 1 and 65535, whose unit is frame number
	Error-frame second event ranges between 1 and 900, whose unit is second
	Error-CRC event ranges between 1 and 65535, whose unit is frame number

Default

The default value of the error-signal period event is 1

The default value of the error-frame event is 1

The default value of the error-frame period event is 1

The default value of the error-frame second event is 1

The default value of the error-CRC event is 10

Command Mode

Port configuration mode

Usage Guidelines

After the low threshold of an event is configured and the locally-received event exceeds the low threshold, the Event Notification OAM packet will be transmitted to notify the peer terminal

Example

The following example shows how to set the low threshold of the error-frame event to **10** on interface GigaEthernet0/2.

Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold low 10

46.6 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window

Syntax

ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window *value*

To configure the size of the round-query window for link monitoring, run the previous command

Parameter

Parameter	Description
Value	The error-signal period event ranges between 10 and 600 on GigaEthernet and ranges between 1 and 60 on FastEthernet. The unit is 100M signals The error-frame event ranges between 1 and 60, whose unit is second The error-frame period event ranges between 100 and 6000 on GigaEthernet and ranges between 10 and 600 on FastEthernet. The unit is 14881 frames Error-frame second event ranges between 10 and 900, whose unit is second The error-CRC event ranges between 1 and 180, whose unit is second

Default

The default value of the error-signal period event is 10 on GigaEthernet and is 1 on FastEthernet

The default value of the error-frame event is 1

The default value of the error-frame period event is 100 on GigaEthernet and is 10 on FastEthernet

The default value of the error-frame second event is 60

The default value of the error-CRC event is 1

Command Mode

Port configuration mode

Usage Guidelines

None

Example

The following example shows how to set the window of the error-frame period event to **50** on interface GigaEthernet0/2

Switch_config_g0/2#ethernet oam link-monitor symbol-period window 50

46.7 ethernet oam link-monitor high-threshold action

Syntax

ethernet oam link-monitor high-threshold action error-disable-interface

[**no**] **ethernet oam link-monitor high-threshold action**

To configure the link-monitor trigger event with the high threshold, run **ethernet oam link-monitor high-threshold action error-disable-interface**.

Parameter

None

Default

The high-threshold trigger event does not exist by default

Command Mode

Port configuration mode

Usage Guidelines

After the high threshold of an event and **ethernet oam link-monitor high-threshold action error-disable-interface** are configured, the local port enters the **errdisabled** state when the local port receives the high threshold of the event

Example

The following example shows how to set the high-threshold trigger event on interface GigaEthernet 0/2 to **error-disable-interface**

Switch_config_g0/2#ethernet oam link-monitor high-threshold action error-disable-interface

46.8 ethernet oam link-monitor negotiation-supported

Syntax

[**no**] **ethernet oam link-monitor negotiation-supported**

To configure the link-monitor negotiation, run **ethernet oam link-monitor negotiation-supported**

Parameter

None

Default

Link-monitor negotiation is supported

Command Mode

Port configuration mode

Usage Guidelines

Devices support link monitoring. However, if the third-party devices do not support link monitoring, devices automatically do not support link monitoring during OAM Discovery and the OAM connection can be established through the third-party devices in this case. Otherwise, when the link-monitor negotiation is not configured, devices mandatorily support the link-monitor function, but the OAM connection cannot be created if the third-party devices do not support the link-monitor function

Example

The following example shows that the link-monitor function is not supported on interface GigaEthernet 0/2.

Switch_config_g0/2#no ethernet oam link-monitor negotiation-supported

46.9 clear ethernet oam statistics

Syntax

clear ethernet oam statistics [interface intf-type intf-id**]**

To clear the OAM statistics information, run the previous command

Parameter

Parameter	Description
intf-id	Designates an interface. If an interface is not designated, the OAM statistics information on all interfaces will be deleted

Default

None

Command Mode

Privileged mode

Usage Guidelines

After this command is run, the following statistics information (type-classified packet numbering information, link-event statistics information and remote trouble statistics information) is deleted meanwhile

Example

The following example shows how to clear the OAM statistics information on interface GigaEthernet 0/2

Switch#clear ethernet oam statistics interface g0/2

46.9.1 show ethernet oam discovery

Syntax

show ethernet oam discovery interface [intf-type intf-id]

To display the OAM discovery information on all interfaces or a designated interface, run the previous command.

Parameter

Parameter	Description
intf-id	Displays the Discovery information on the designated interface or on all protocol-up ports and enables the Discovery information on the OAM interface

Default

None

Usage Guidelines

None

Example

The following example shows how to display the OAM discovery information on interface GigaEthernet 0/2.

Switch_config_g0/2#show ethernet oam discovery interface g0/2

GigaEthernet0/2

Local Info TLV

PDU revision: 1

Loopback status: LB_DISABLED

OAM configurations field:

Mode : active

Unidirection : not supported

Remote loopback : supported

Link Events : supported

Variable retrieval: not supported

Mtu size: 1500

OUI: 00e00f

Remote Info TLV

MAC address: 001b.0d9c.e703

PDU revision: 0

OAM configurations field:

Mode : active

Unidirection : not supported

Remote loopback : not supported

Link Events : supported

Variable retrieval: not supported

Mtu size: 1500

OUI: 00000c

46.10 show ethernet oam statistics {pdu | link-monitor | remote-failure}

Syntax

show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id**]**

To display the OAM statistics information on a designated interface or all interfaces, run the previous command

Parameter

Parameter	Description
intf-id	Displays the statistics information on the designated interface or on all protocol-up ports and enables the statistics information on the OAM interface

Default

None

Usage Guidelines

None

Example

The following example shows how to display the classified OAM packet numbering information on interface GigaEthernet 0/2

Switch#show ethernet oam statistics pdu interface g0/2

GigaEthernet0/2

Counters:

Information OAMPDU Tx : 59

Information OAMPDU Rx : 56

Unique Event Notification OAMPDU Tx : 0

Unique Event Notification OAMPDU Rx : 0

Duplicate Event Notification OAMPDU TX: 0

Duplicate Event Notification OAMPDU RX: 0

Loopback Control OAMPDU Tx : 0

Loopback Control OAMPDU Rx : 0

Variable Request OAMPDU Tx : 0

Variable Request OAMPDU Rx : 0

Variable Response OAMPDU Tx : 0

Variable Response OAMPDU Rx : 0

Organization Specific OAMPDU Tx : 0

Organization Specific OAMPDU Rx : 0

Unsupported OAMPDU Tx : 0

Unsupported OAMPDU Rx : 0

Frames Lost due to OAM : 0

46.11 show ethernet oam configuration

Syntax

show ethernet oam configuration interface [intf-type intf-id]

To display the OAM configuration information on all interfaces or a designated interface, run **show ethernet oam configuration interface [intf-type intf-id]**

Parameter

Parameter	Description
intf-id	Displays the OAM configuration information on the designated interface or on all protocol-up ports and enables the configuration information on the OAM interface

Default

None

Usage Guidelines

None

Example

The following example shows how to display the OAM configuration information on interface GigaEthernet 0/2.

Switch#show ethernet oam configuration interface g0/2

GigaEthernet0/2

General

Admin state : enabled

Mode : active

PDU max rate : 10 packets/second

PDU min rate : 1 seconds/packet

Link timeout : 1 seconds

High threshold action: no action

Remote Failure

Link fault action : no action

Dying gasp action : no action

Critical event action: no action

Remote Loopback

Is supported : supported

Loopback timeout : 2

Link Monitoring

Negotiation : supported

Status : on

Errored Symbol Period Event

Window : 10 * 100M symbols

Low threshold : 1 error symbol(s)

High threshold : none

Errored Frame Event

Window : 1 seconds

Low threshold : 1 error frame(s)

High threshold : none

Errored Frame Period Event

Window : 100 * 14881 frames

Low threshold : 1 error frame(s)

High threshold : none

Errored Frame Seconds Summary Event

Window : 60 seconds

Low threshold : 1 error second(s)

High threshold : none

Errored CRC Frames Event

Window : 1 seconds

Low threshold : 10 error frame(s)

High threshold : none

46.12 show ethernet oam runtime

Syntax

show ethernet oam runtime interface [intf-type intf-id**]**

To display the OAM running information on all interfaces or a designated interface, run the previous command

Parameter

Parameter	Description
intf-id	Displays the Runtime information on the designated interface or on all protocol-up ports and enables the Runtime information on the OAM interface

Default

None

Usage Guidelines

None

Example

The following example shows how to display the OAM Runtime information on interface GigaEthernet 0/2

Switch#show ethernet oam runtime interface g0/2

GigaEthernet0/2

Runtime Settings:

---

local_pdu : NOT_WORKING

local_mux : FWD

local_par : FWD

local_link_status : OK

local_satisfied : FALSE

local_stable : FALSE

pdu_cnt : 10

pdu_timer : stopped

lost_link_timer : stopped

remote_state_valid: FALSE

remote_stable : FALSE

remote_evaluating : FALSE

Discovery State Machine:

Last 10 state transition recorded: INACTIVE -> FAULT -> ACTIVE_SEND_LOCAL -> SEN

D_LOCAL_REMOTE -> SEND_LOCAL_REMOTE_OK -> SEND_ANY -> INACTIVE

Chapter 47 Optical Port Additional Function Configuration Commands

47.1 Configure the DDM Function

47.1.1 ddm enable

Syntax

To enable DDM detection function of the optical port, use **ddm enable** command

ddm enable

Parameter

Parameter	Description
enable	Enable optical port ddm detection

Default

None

Command mode

Global configuration mode

Example

ddm enable

47.1.2 no ddm

Syntax

no ddm

To disable DDM detection function of the optical port, use **no ddm** command

Parameter

None

Default

None

Command mode

Global configuration mode

Example

The following example shows how to disable DDM detection function of the optical port.

Switch-config#no ddm

47.2 Configure the single-fiber transceiver function of the optical port

47.2.1 single-fiber one-way

Syntax

To configure the transceiver function of the optical fiber, use the following command

single-fiber one-way <tx|rx>

no single-fiber

Parameter

Parameter	Description
tx	Configure the port to work in single-fiber transmission mode
rx	Configure the port to work in single-fiber receiving mode

Default

None

Command mode

None

Example

The following example shows how to configure single-fiber transmission mode isolation on port g0/1

Switch_config_g0/1#single-fiber one-way tx

The following example shows how to cancel single fiber mode of port g0/1

Switch_config_g0/1#no single-fiber

47.3 Optical module auto-configuration

47.3.1 fiber-auto-config

Syntax

To enable the storm control function of the port, use the following command

fiber-auto-config {**full**}

Parameter

Parameter	Description
full	When switching to gigabit mode mode, configure in forced mode
None	When switching to gigabit mode, configure in adaptive mode

Default

None

Command mode

Interface configuration mode

Example

The following example enables the optical module auto-configuration on interface g0/1, and use the adaptive mode in gigabit mode

Switch_config#interface g0/1

Switch_config_g0/1#fiber-auto-config

The following example enables the optical module auto-configuration on interface g0/1, and use the forced mode in gigabit mode.

Switch_config#interface g0/1

Switch_config_g0/1#fiber-auto-config full

The following example cancels optical module auto-configuration of interface g0/1.

Switch_config#interface g0/1

Switch_config_g0/1#no fiber-auto-config

Note:

When using a Gigabit optical conversion module that supports 10/100/1000M mode, you must configure this command in adaptive mode. When using a Gigabit optical conversion module that only supports the 1000M mode, you do not need to configure this command

Chapter 48 OSPFv3 Configuration Commands

48.1 area default-cost

Syntax

To specify the cost of the default summary route in the NSSA or STUB area, run the first one of the following two commands:

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost** *cost*

Parameter

Parameter	Description
area-id	Means the ID of the NSSA or STUB area.
cost	Means the cost of the default summary route.

Default value

The default value is 1

Command mode

Routing configuration mode

Usage guidelines

The command is helpful only when it is used on the boundary router connecting the NASSA area or the STUB area

After the area stub default-information-originate command is configured, the cost configured by this command will be used in LSA to set the corresponding cost

Example

The following example shows how to set the default cost of stub domain 36.0.0.0 to 20:

interface vlan 1

ipv6 add 2001::1/64

ipv6 ospf 1 area 36.0.0.0

!

router ospfv3 1

router-id 2.2.2.2

area 36.0.0.0 stub

area 36.0.0.0 default-cost 20

Related command

area nssa

area stub

48.2 area nssa

Syntax

To configure a NSSA area, run the first one of the following two commands:

area *area-id* **nssa** [**default-information-originate** [**metric** *value*] [**metric-type** {1 | 2}]] [**interval** *value*] [**no-redistribute**] [**no-summary**] [**range** {*ipv6-prefix/prefix-length*} [advertise | not-advertise]] [**translator** {always|candidate}]

no area *area-id* **nssa** [**default-information-originate** [**metric** *value*] [**metric-type** {1 | 2}]] [**interval** *value*] [**no-redistribute**] [**no-summary**] [**range** {*ipv6-prefix/prefix-length*} [advertise | not-advertise]] [**translator** {always|candidate}]

Parameter

Parameter	Description
area-id	Sets the ID of the NSSA area. It can be a decimal number or an IP address
default-information-originate	Means to send the default route to the NSSA area. After this command is configured, if it is a non-ABR in the NSSA area, it needs an IPv6 default route on the device before sending the default route to the NSSA area; on the ABR, regardless of whether there is an IPv6 default route on the device, it will be sent to NSSA Area sending default route
metric *value*	Stands for the cost of the default route, which ranges from 1 to 16777214
metric-type *{1 / 2}*	Means the cost type of the default route
interval *value*	Means the stable time of the NSSA translator role, which ranges from 1 to 65535
no-redistribute	Means not to redistribute a route to the NSSA area
no-summary	Forbids the ABR router to send the summary link to the NSSA area
range	Means to conduct summary when type-7 LSA is translated into type-5 LSA
translator	Stands for the NSSA translator role; if the parameter "always" is used, it means it is always the translator, and if it is the parameter "candidate", it means it can be chosen as a translator

Default value

Non-NSSA area

Command mode

Routing configuration mode

Usage guidelines

All routers and access servers in the NSSA area will be configured by the area nssa command

To decrease the number of LSA's, you can run no summary on the ABR router to forbid the summary LSA to enter the NSSA area

The parameter "no-distribute" is always used for ABR and its purpose is to stop redistributed routes from being sent to the NSSA area

Example

The following example shows how to set the NSSA area of 36.0.0.0:

interface vlan 1

ipv6 address 2001::1/64

ipv6 ospf 1 area 36.0.0.0

!

router ospfv3 1

router-id 2.2.2.2

area 36.0.0.0 nssa

!

Related command

area stub

48.3 area range

Syntax

To summarize the routes at the field boundary, run **area** *area-id* **range**. To cancel the previous settings, run **no area** *area-id* **range**

area *area-id* **range {***ipv6-prefix /prefix-length***} [advertise | not-advertise]**

no area *area-id* **range {***ipv6-prefix /prefix-length***}**

Parameter

Parameter	Description
area-id	Means the fields where the fields will be summarized. It can be a decimal number or an IPv6 address
ipv6-prefix	Means the prefix of the IPv6 address
prefix-length	Means the length of the IPv6 address' prefix
advertise	Means that the routes are released after they are summarized

not-advertise	Means that the routes are not released after they are summarized

Default value

The command has no effect by default

Command mode

Routing configuration mode

Usage guidelines

The **area range** command is not run on the ABR router, enabling ABR to be broadcast to other routers through a summary route. In this way, the route of the field boundary is miniatured. As to the outside of the area, each address range has only one summary route

The command can be configured on the routers in multiple areas, and OSPF, hence, can summarize many address ranges

Example

The following example shows how to set the prefix of the summarized IPv6 address in area 1, 2001:0DB8:0:1::/64:

interface vlan 1

ipv6 address 2001::1/64

ipv6 ospf 1 area 1

!

router ospfv3 1

router-id 192.168.255.5

area 1 range 2001:0DB8:0:1::/64

48.4 area stub

Syntax

To configure a STUB area, run the first one of the following two commands. To cancel the configuration, run the other command

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

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

Parameter

Parameter	Description
area-id	Sets the ID of the STUB area. It can be a decimal number or an IP address

no-summary	Forbids the ABR router to send the summary link to the STUB area

Default value

Non-stub area

Command mode

Routing configuration mode

Usage guidelines

All routers and access servers in the STUB area will be configured by the **area stub** command. The ABR router adopts the **default-cost** option to set the cost from the internal router to the STUB area

The **default-cost** subcommand is only used on the domain border router connected to the stub area to set the cost of the convergence route generated by the domain border router to reach the stub area

To decrease the number of LSA's, you can run **no summary** on the ABR router to forbid the summary LSA to enter the STUB area

Example

The following example shows how to set the STUB area of 36.0.0.0:

```
interface vlan 1
    ipv6 address 2001::1/64
    ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
    router-id 2.2.2.2
    area 36.0.0.0 stub
!
```

Related command

area nssa

48.5 area virtual-link

Syntax

To configure a virtual link, run the first one of the following two commands

area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*]

no area *area-id* **virtual-link** *neighbor-ID*

Parameter

Parameter	Description
area-id	Specifies the transit-area of the virtual link

neighbor-id	OSPF router ID of the peer router of virtual link
dead-value	Stands for the interval for the local router to regard that the neighbor dies, whose unit is second. The values configured at the two terminals of the virtual link must be same
hello-value	Stands for the interval for the router to transmit the HELLO packet on the virtual link, whose unit is second. The values configured at the two terminals of the virtual link must be same
retrans-value	Interval for the router to transmit the **re-transmit** packet on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same
dly-value	Delay value which is reported by the router to LSA on the virtual link, whose unit is second The values configured at the two terminals of the virtual link must be same. The values configured at the two terminals of the virtual link must be same

Default value

The virtual link is not configured

The default values of other parameters are shown in the following:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s

Command mode

Routing configuration mode

Usage guidelines

In order to create a virtual link, you have to perform configuration at the two terminals of the virtual link. If only one terminal need be configured, the virtual link cannot function

The **area-id** parameter cannot be zero because the transit area of the virtual link must not be the backbone area. The area-id configured at the two terminals of the virtual link must be same

Parameters configured at the two terminals of the virtual link must be same

After the virtual link is created (the neighborhood is in the FULL state), the virtual link works in the Demand Circuit mode, that is, the periodical Hello packet and the LSA refresh packet are not transmitted

You can run no **area** ***area-id*** **virtual-link** ***neighbor-ID*** to cancel the previous configuration of the virtual link

You also can run **show ip ospf virtual-link** to check the state of the virtual link

Example

The following example shows how to create a virtual link between router A and router B

Configuration of Switch A(router-id: 200.200.200.1)

!

interface vlan 1

ipv6 address 2001::1/64

ipv6 ospf 1 area 1

!

router ospfv3 1

router-id 200.200.200.1

area 1 virtual-link 200.200.200.2

!

Configuration of Switch B(router-id: 200.200.200.2):

!

interface vlan 1

ipv6 address 2001::2/64

ipv6 ospf 1 area 1

!

router ospfv3 1

router-id 200.200.200.2

area 1 virtual-link 200.200.200.1

!

Related command

show ipv6 ospf virtual-link

48.6 debug ipv6 ospf

Syntax

To open all debugging switches of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf

no debug ipv6 ospf

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

This command can be used to collect all debugging information about the OSPFv3 for the R&D engineers and technical support staff

Example

Switch# debug ipv6 ospf

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA(0x38110c0) originated

VLINK[VLINK1]: local address is 101::1VLINK[VLINK1]: peer 200.200.200.2 link upLSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link FastEthernet0/0

LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Link-LSA(0x381ec40) originated

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x381ec20) originated

IFSM[FastEthernet0/0]: Down (InterfaceUp)

IFSM[FastEthernet0/0]: Status change Down -> Waiting

SPF[0.0.0.0]: Calculation timer scheduled [delay 5 secs]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x38297e0) originated

IFSM[VLINK1]: Down (InterfaceUp)

IFSM[VLINK1]: Status change Down -> Point-To-Point

ROUTER[1]: Change status to ABR

IFSM[FastEthernet0/0]: Hello timer expire

Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)

OSPFv3 Header

Version 3 Type 1 (Hello) Packet length 36

Router ID 200.200.200.1

Area ID 0.0.0.1

Checksum 0x0000 Instance ID 0

OSPFv3 Hello

Interface ID 4

RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)

HelloInterval 10 RtrDeadInterval 40

DRouter 0.0.0.0 BDRouter 0.0.0.0

Neighbors 0

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

……

48.7 debug ipv6 ospf events

Syntax

To enable the event debug switch of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf events {abr|asbr|vlink|os|router}

no debug ipv6 ospf events { abr|asbr|vlink|os|router }

Parameter

Parameter	Description
abr	Opens the state change debug switch of ABR
asbr	Opens the state change debug switch of ASBR
vlink	Opens the state change debug switch of the virtual link
os	Opens the state change debug switch of socket
router	Opens the debug switch of OSPF

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by the command, you can check the OSPF port and the neighbor trigger event

Example

Switch# debug ip ospf events

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

ROUTER[1]: Change status to ABR

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

VLINK[VLINK1]: peer 200.200.200.2 link downROUTER[1]: Change status to non-ABR

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

ROUTER[Process:1]: GC timer expire

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_TIMER.

ROUTER[Process:1]: GC timer expire

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_SOCKET.

join AllDRouters on FastEthernet0/0OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

OSPF6D: Received ospfv3 message: OSPFV3_MSG_RCV_EVENT.

……

48.8 debug ipv6 ospf ifsm

Syntax

To enable the state machine's debug switch of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf ifsm {status|events|timers}

no debug ipv6 ospf ifsm {status|events|timers}

Parameter

Parameter	Description
status	Opens the state debug switch of the interface state machine
events	Opens the event debug switch of the interface state machine
timers	Opens the timer debug switch of the interface state machine

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by the command, you can check the whole process of the state machine of the OSPF interface

Example

Switch # debug ipv6 ospf ifsm

IFSM[VLINK1]: Down (InterfaceUp)

IFSM[VLINK1]: Status change Down -> Point-To-Point

IFSM[FastEthernet0/0]: Down (InterfaceUp)

IFSM[FastEthernet0/0]: Status change Down -> Waiting

IFSM[FastEthernet0/0]: Hello timer expire

IFSM[VLINK1]: Hello timer expire

IFSM[VLINK1]: ifsm_ignore called

IFSM[VLINK1]: Point-To-Point (NeighborChange)

IFSM[FastEthernet0/0]: ifsm_ignore called

IFSM[FastEthernet0/0]: Waiting (NeighborChange)

IFSM[VLINK1]: LS ack timer expire

IFSM[VLINK1]: LS ack timer expire

IFSM[VLINK1]: Point-To-Point (InterfaceDown)

IFSM[VLINK1]: Status change Point-To-Point -> Down

IFSM[VLINK1]: ifsm_ignore called

IFSM[VLINK1]: Down (NeighborChange)

IFSM[FastEthernet0/0]: Hello timer expire

IFSM[FastEthernet0/0]: Hello timer expire

IFSM[FastEthernet0/0]: Hello timer expire

IFSM[FastEthernet0/0]: Wait timer expire

IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.2

IFSM[FastEthernet0/0]: DR-Election[1st]: DR 200.200.200.2

IFSM[FastEthernet0/0]: Waiting (WaitTimer)

IFSM[FastEthernet0/0]: Status change Waiting -> DROther

IFSM[VLINK1]: Down (InterfaceUp)

IFSM[VLINK1]: Status change Down -> Point-To-Point

IFSM[FastEthernet0/0]: DR-Election[1st]: Backup 200.200.200.1

IFSM[FastEthernet0/0]: DR-Election[1st]: DR 200.200.200.2

IFSM[FastEthernet0/0]: DR-Election[2nd]: Backup 200.200.200.1

IFSM[FastEthernet0/0]: DR-Election[2nd]: DR 200.200.200.2

IFSM[FastEthernet0/0]: DROther (NeighborChange)

IFSM[FastEthernet0/0]: Status change DROther -> Backup

IFSM[FastEthernet0/0]: Hello timer expire

IFSM[FastEthernet0/0]: LS ack timer expire

IFSM[VLINK1]: Hello timer expire

IFSM[FastEthernet0/0]: LS ack timer expire

IFSM[VLINK1]: Point-To-Point (InterfaceDown)

IFSM[VLINK1]: Status change Point-To-Point -> Down

IFSM[VLINK1]: Down (InterfaceUp)

IFSM[VLINK1]: Status change Down -> Point-To-Point

IFSM[FastEthernet0/0]: LS ack timer expire

IFSM[VLINK1]: Hello timer expire

……

48.9 debug ipv6 ospf lsa

Syntax

To enable the LSA-related debug switch of the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf lsa { generate|flooding|install|maxage|refresh}

no debug ipv6 ospf lsa { generate|flooding|install|maxage|refresh}

Parameter

Parameter	Description
generate	Opens the debug switch of LSA create
flooding	Opens the debug switch of LSA exchange

install	Opens the debug switch of LSA installation
maxage	Opens the debug switch of LSA timeout
refresh	Opens the debug switch of LSA-Refresh

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by the command, you can browse the operation that OSPF performs to LSA and related events

Example

Switch # debug ipv6 ospf lsa

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA(0x3824ba0) originated

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding to neighbor[200.200.200.2]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3819be0) originated

LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Install Link-LSA to Link FastEthernet0/0

LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Link(FastEthernet0/0):Type(0x0008):0.0.0.4:200.200.200.1 *]: Link-LSA(0x3819bc0) originated

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA(0x3824740) originated

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: instance(0x380bf60) created with Link State Update

LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: instance(0x38246c0) created with Link State Update

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: flood started

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: consider flooding through interface[VLINK1]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: consider flooding to neighbor[200.200.200.2]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: neighbor is not Full state

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.2]: Install Router-LSA to Area 0.0.0.0

LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: flood started

LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: consider flooding through interface[VLINK1]

LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: consider flooding to neighbor[200.200.200.2]

LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: neighbor is not Full state

LSA[Area(0.0.0.0):Type(0x2003):0.0.0.1:200.200.200.2]: Install Inter-Area-Prefix-LSA to Area 0.0.0.0

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.0

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding to neighbor[200.200.200.2]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: added to neighbor[200.200.200.2]'s retransmit-list

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: sending update to interface[VLINK1]

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA refreshed

OSPFv3 LSA Header

LS age 0

LS type 0x2001 (Router-LSA)

Advertising Router 200.200.200.1

Link State ID 0.0.0.0

LS sequence number 0x80000002

LS checksum 0x5ff7

length 40

LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[VLINK1]

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Install Router-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2001):0.0.0.0:200.200.200.1 *]: Router-LSA refreshed

OSPFv3 LSA Header

LS age 0

LS type 0x2001 (Router-LSA)

Advertising Router 200.200.200.1

Link State ID 0.0.0.0

LS sequence number 0x80000002

LS checksum 0x5382

length 24

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Install Intra-Area-Prefix-LSA to Area 0.0.0.1

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: consider flooding through interface[FastEthernet0/0]

LSA[Area(0.0.0.1):Type(0x2009):0.0.0.1:200.200.200.1 *]: Intra-Area-Prefix-LSA refreshed

OSPFv3 LSA Header

LS age 0

LS type 0x2009 (Intra-Area-Prefix-LSA)

Advertising Router 200.200.200.1

Link State ID 0.0.0.1

LS sequence number 0x80000002

LS checksum 0x3631

length 64

……

48.10 debug ipv6 ospf nfsm

Syntax

To enable the state machine's debug switch of the OSPFv3 neighbor, run the first one of the following two commands:

debug ipv6 ospf nfsm {status|events|timers}

no debug ipv6 ospf nfsm {status|events|timers}

Parameter

Parameter	Description
status	Opens the state debug switch of the neighbor state machine
events	Opens the event debug switch of the neighbor state machine
timers	Opens the timer debug switch of the neighbor state machine

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by the command, you can check the whole process of the OSPF neighbor's state machine

Example

Switch # debug ipv6 ospf nfsm

NFSM[200.200.200.2-00000004]: Full (HelloReceived)

NFSM[200.200.200.2-00000004]: nfsm_ignore calledNFSM[200.200.200.2-00000004]: Full (2-WayReceived)

NFSM[200.200.200.2-00000004]: Down (HelloReceived)

NFSM[200.200.200.2-00000004]: Status change Down -> Init

NFSM[200.200.200.2-00000004]: nfsm_ignore called

NFSM[200.200.200.2-00000004]: Init (1-WayReceived)

NFSM[200.200.200.2-00000004]: Init (HelloReceived)

NFSM[200.200.200.2-00000004]: Init (2-WayReceived)

NFSM[200.200.200.2-00000004]: Status change Init -> 2-Way

NFSM[200.200.200.2-00000004]: 2-Way (HelloReceived)

NFSM[200.200.200.2-00000004]: nfsm_ignore called

NFSM[200.200.200.2-00000004]: 2-Way (2-WayReceived)

NFSM[200.200.200.2-00000004]: 2-Way (AdjOK?)

NFSM[200.200.200.2-00000004]: Status change 2-Way -> ExStar

tNFSM[200.200.200.2-00000004]: ExStart (HelloReceived)

NFSM[200.200.200.2-00000004]: nfsm_ignore called

NFSM[200.200.200.2-00000004]: ExStart (2-WayReceived)

NFSM[200.200.200.2-00000004]: DD Retransmit timer expire

NFSM[200.200.200.2-00000004]: ExStart (NegotiationDone)

NFSM[200.200.200.2-00000004]: Status change ExStart -> Exchange

NFSM[200.200.200.2-00000004]: Exchange (ExchangeDone)

NFSM[200.200.200.2-00000004]: Status change Exchange -> Loading

NFSM[200.200.200.2-00000004]: nfsm_ignore called

NFSM[200.200.200.2-00000004]: Loading (LoadingDone)

NFSM[200.200.200.2-00000004]: Status change Loading -> Full

NFSM[200.200.200.2-80000001]: Down (HelloReceived)

NFSM[200.200.200.2-80000001]: Status change Down -> Init

NFSM[200.200.200.2-80000001]: Init (2-WayReceived)

NFSM[200.200.200.2-80000001]: Status change Init -> ExStart

NFSM[200.200.200.2-80000001]: ExStart (NegotiationDone)

NFSM[200.200.200.2-80000001]: Status change ExStart -> Exchange

NFSM[200.200.200.2-80000001]: Exchange (ExchangeDone)

NFSM[200.200.200.2-80000001]: Status change Exchange -> Loading

NFSM[200.200.200.2-80000001]: nfsm_ignore called

NFSM[200.200.200.2-80000001]: Loading (LoadingDone)

NFSM[200.200.200.2-80000001]: Status change Loading -> Full

NFSM[200.200.200.2-00000004]: Full (HelloReceived)

NFSM[200.200.200.2-00000004]: nfsm_ignore called

NFSM[200.200.200.2-00000004]: Full (2-WayReceived)

NFSM[200.200.200.2-00000004]: Full (AdjOK?)

NFSM[200.200.200.2-00000004]: LS update timer expire

NFSM[200.200.200.2-80000001]: LS update timer expire

NFSM[200.200.200.2-00000004]: LS update timer expire

NFSM[200.200.200.2-80000001]: LS update timer expire

NFSM[200.200.200.2-80000001]: Full (HelloReceived)

NFSM[200.200.200.2-80000001]: nfsm_ignore called

NFSM[200.200.200.2-80000001]: Full (2-WayReceived)

NFSM[200.200.200.2-00000004]: Full (HelloReceived)

NFSM[200.200.200.2-00000004]: nfsm_ignore called

NFSM[200.200.200.2-00000004]: Full (2-WayReceived)

NFSM[200.200.200.2-00000004]: LS update timer expire

NFSM[200.200.200.2-80000001]: LS update timer expire

……

48.11 debug ipv6 ospf nsm

Syntax

To open the debug switch of information transmission between the IPv6 routing table's management module and the OSPFv3 module, run the first one of the following two commands:

debug ipv6 ospf nsm { redistribute | interface }

no debug ipv6 ospf nsm { redistribute | interface }

Parameter

Parameter	Description
redistribute	Opens the debug switch of routing information forwarding
interface	Opens the debug switch of interface events

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by this command, you can browse information exchange between OSPF and routing management module

Example

Switch # debug ipv6 ospf nsm

Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message

Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message

Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message

Sep 17 16:43:53 OSPFv3: Received [NSM_MSG_ROUTE_CHG_NOTIFY:NSM_REDISTRIBUTE_DEL] message

Sep 17 16:43:53 OSPFv3: Receive [NSM_MSG_GLBL_ENAIPV6] message

……

48.12 debug ipv6 ospf packet

Syntax

To enable the debug switch of OSPFv3 transmission and reception, run the first one of the following two commands:

debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack |detail}

no debug ipv6 ospf packet { hello|dd|ls-request|ls-update|ls-ack|detail }

Parameter

Parameter	Description
hello	Opens the debug switch of Hello packets

dd	Opens the debug switch of DD packets
ls-request	Opens the debug switch of IS-REQUEST packets
ls-update	Opens the debug switch of IS-Update packets
ls-ack	Opens the debug switch of IS-Ack packets
detail	Observes the details of packets

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by the command, you can check the exchange of the OSPF packets

Example

```
Switch # debug ipv6 ospf packet
Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)
OSPFv3 Header
  Version 3    Type 1 (Hello)    Packet length 40
  Router ID 200.200.200.1
  Area ID 0.0.0.1
  Checksum 0x0000    Instance ID 0
OSPFv3 Hello
  Interface ID 4
  RtrPriority 1    Options 0x000013 (-|R|-|-|E|V6)
  HelloInterval 10    RtrDeadInterval 40
  DRouter 200.200.200.2    BDRouter 200.200.200.1
  # Neighbors 1
    Neighbor 200.200.200.2
Packet[RECV]: src(101::2) -> dst(101::1)
OSPFv3 Header
  Version 3    Type 1 (Hello)    Packet length 40
```

```
    Router ID 200.200.200.2
    Area ID 0.0.0.0
    Checksum 0x5774    Instance ID 0
  OSPFv3 Hello
    Interface ID 2147483649
    RtrPriority 1    Options 0x000013 (-|R|-|-|E|V6)
    HelloInterval 10    RtrDeadInterval 40
    DRouter 0.0.0.0    BDRouter 0.0.0.0
    # Neighbors 1
      Neighbor 200.200.200.1
  RECV[Hello]: Neighbor(200.200.200.2) declare 0.0.0.0 as DR, 0.0.0.0 as Backup
  Packet[SEND]: src(101::1) -> dst(101::2)
  OSPFv3 Header
    Version 3    Type 1 (Hello)    Packet length 40
    Router ID 200.200.200.1
    Area ID 0.0.0.0
    Checksum 0x0000    Instance ID 0
  OSPFv3 Hello
    Interface ID 2147483649
    RtrPriority 1    Options 0x000013 (-|R|-|-|E|V6)
    HelloInterval 10    RtrDeadInterval 40
    DRouter 0.0.0.0    BDRouter 0.0.0.0
    # Neighbors 1
      Neighbor 200.200.200.2
  Packet[RECV]: src(fe80::2e0:fff:fe26:a8) -> dst(ff02::5)
  OSPFv3 Header
    Version 3    Type 1 (Hello)    Packet length 40
    Router ID 200.200.200.2
    Area ID 0.0.0.1
    Checksum 0xa8a8    Instance ID 0
  OSPFv3 Hello
```

Interface ID 4

RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)

HelloInterval 10 RtrDeadInterval 40

DRouter 200.200.200.2 BDRouter 200.200.200.1

Neighbors 1

Neighbor 200.200.200.1

RECV[Hello]: Neighbor(200.200.200.2) declare 200.200.200.2 as DR, 200.200.200.1 as Backup

Packet[SEND]: src(fe80:4::2e0:fff:fe26:2d98) -> dst(ff02::5)

OSPFv3 Header

Version 3 Type 1 (Hello) Packet length 40

Router ID 200.200.200.1

Area ID 0.0.0.1

Checksum 0x0000 Instance ID 0

OSPFv3 Hello

Interface ID 4

RtrPriority 1 Options 0x000013 (-|R|-|-|E|V6)

HelloInterval 10 RtrDeadInterval 40

DRouter 200.200.200.2 BDRouter 200.200.200.1

Neighbors 1

Neighbor 200.200.200.2

……

48.13 debug ipv6 ospf route

Syntax

To enable the debug switch of OSPFv3 routing information, run the first one of the following two commands:

debug ipv6 ospf route { ase|install|spf|ia|nssa}

no debug ipv6 ospf route { ase|install|spf|ia|nssa }

Parameter

Parameter	Description
ase	Opens the debug switch of exterior routing calculation

install	Opens the debug switch of routing installation procedure
spf	Opens the debug switch of SPF calculation
ia	Opens the debug switch of between-domain routing calculation
nssa	Opens the debug switch of nssa type exterior routing calculation

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by the command, you can browse the calculation, deletion and addition of OSPF routes

Example

Switch # debug ipv6 ospf route

Route[IA:0.0.0.0]: No SPF tree, schedule SPF calculationSPF[0.0.0.1]: SPF calculation timer expire

SPF[0.0.0.1]: SPF calculation (1st STAGE)

SPF[0.0.0.1]: Vertex[200.200.200.1-0.0.0.0]

SPF[0.0.0.1]: SPF calculation (2nd STAGE)

SPF[0.0.0.1]: SPF calculation (END)

Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsRoute[IA:0.0.0.1]: Cleanup IA route because of no ABRsSPF[0.0.0.1]: Calculation completed [0.170000 sec]

SPF[0.0.0.1]: Calculation timer scheduled [delay 9 secs]

SPF[0.0.0.1]: SPF calculation timer expire

SPF[0.0.0.1]: SPF calculation (1st STAGE)

SPF[0.0.0.1]: Vertex[200.200.200.1-0.0.0.0]

SPF[0.0.0.1]: SPF calculation (2nd STAGE)

SPF[0.0.0.1]: SPF calculation (END)

Route[IA:0.0.0.1]: Cleanup IA route because of no ABRsSPF[0.0.0.1]: Calculation completed [0.180000 sec]

SPF[0.0.0.1]: Calculation timer scheduled [delay 10 secs]

SPF[0.0.0.0]: Calculation timer scheduled [delay 5 secs]

Route[IA:0.0.0.1]: 888::/64 calculating Network routeRoute[IA:0.0.0.1]: 888::/64 Can't find route to ABR (200.200.200.2)Route[IA:0.0.0.0]: No SPF tree, schedule SPF calculationSPF[0.0.0.0]: SPF calculation timer expire

SPF[0.0.0.0]: SPF calculation (1st STAGE)

SPF[0.0.0.0]: Vertex[200.200.200.1-0.0.0.0]

SPF[0.0.0.0]: Link[0] (200.200.200.2-128.0.0.1): Virtual-Link

SPF[0.0.0.0]: Calculate nexthop for (200.200.200.2-0.0.0.0)

Route[0.0.0.0:SPF]: ADD Stub Route for (200.200.200.2)SPF[0.0.0.0]: Vertex[200.200.200.2-0.0.0.0]

SPF[0.0.0.0]: Link[0] (200.200.200.1-128.0.0.1): Virtual-Link

SPF[0.0.0.0]: LSA[Area(0.0.0.0):Type(0x2001):0.0.0.0:200.200.200.1 *] is already in SPF tree

SPF[0.0.0.0]: SPF calculation (2nd STAGE)

SPF[0.0.0.0]: SPF calculation (END)

SPF[0.0.0.0]: Calculation completed [0.580000 sec]

……

48.14 default-information originate

Syntax

To introduce the default route to the OSPFv3 routing domain, run the following command:

default-information originate [always | metric *value* **| metric-type** {1 | 2} **| tag** *tag*]

no default-information originate

Parameter

Parameter	Description
Always	Generates and releases an ASE-LSA, which describes the default route, or just releases it out if the default route exists in the routing table
metric value	Stands for the cost of the default route, which ranges from 1 to 16777214
metric-type	Means the cost type of the default route
tag tag	Means the routing identifier, which ranges from 0 to 4294967295

Default value

No default route is introduced

Command mode

Routing configuration mode

Usage guidelines

The redistribute command cannot introduce the default route, and if you want to introduce the default route,

you can use this command

If the **always** parameter is set, no matter whether the default route exists in the current routing table, ASE-LSA, describing the default route, will be released out; if the **always** parameter is not set, ASE-LSA will be released out only when the default route exists in the current routing table

Example

The following example shows how to introduce the default route from the OSPFv3 autonomous system

router ospfv3 1

router-id 2.2.2.2

default-information originate always

Related command

redistribute

48.15 default-metric

Syntax

To set the default weight of the introduced route, run the first one of the following two commands:

default-metric *value*

no default-metric

Parameter

Parameter	Description
value	Stands for the to-be-set route weight, ranging between 1 and 16777214

Default value

The default route weight is 10

Command mode

Routing configuration mode

Usage guidelines

The **default-metric** command is used to set the default routing weight when the route of other routing protocol is guided into the OSPF packet. When the **redistribute** command is used to guide the route of other routing protocol, the default routing weight designated by the **default-metric** command will be guided the specific routing weight will not be specified

Example

The following example shows how to introduce the static route and set the default route weight of other routing protocol to 3:

```
interface vlan 1
ipv6 address 2001::1/64
ipv6 ospf 1 area 36.0.0.0
!
router ospfv3 1
router-id 2.2.2.2
default-metric 3
redistribute static
```

Related command

redistribute

48.16 filter

Syntax

To set the routing filtration table, run **filter**. To resume the default settings, run **no filter**.

filter {**vlan** *vlan-interface-number* | ***}** {**in | out** } {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

no filter {**vlan** *vlan-interface-number* | ***}** {**in | out** }

Parameter

vlan	Vlan interface
vlan-interface-number	Interface number
*	All interfaces
In	Filtrates the received OSPF routes
out	Filters the transmitted routes, which is not for a specific interface but for all interfaces
access-list-name	Name of the IP access control list
access-list-name	Name of the IP access control list
prefix-list-name	Name of the prefix list

Default value

None

Command mode

Routing configuration mode

Example

The following example shows how to filter the received routes according to the mylist ACL.

router ospfv3 1

filter * in access-list mylist

Related command

None

48.17 ipv6 ospf area

Syntax

To enable the OSPFv3 protocol on an interface and specify an area for this interface, run the first one of the following two commands:

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

Parameter

Parameter	Description
process-id	Stands for the OSPF process
area-id	Stands for the OSPF area ID, which is specified by the interface
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

None

Command mode

Interface configuration mode

Example

The following example shows how to enable OSPFv3 process 1 for interface vlan1 and set its area ID to 0.

interface vlan 1

ipv6 address 2001::1/64

ipv6 ospf 1 area 0

!

router ospfv3 1

router-id 2.2.2.2

Related command

None

48.18 ipv6 ospf cost

Syntax

To designate the cost for the OSPFv3 protocol running on the interface, run **ipv6 ospf cost *cost***. To resume the default settings, run **no ipv6 ospf cost**

ipv6 ospf cost *cost* [**instance** *instance-id*]

no ipv6 ospf *cost* *cost* [**instance** *instance-id*]

Parameter

Parameter	Description
cost	Cost for the OSPF protocol, which is an integer between 1 and 65535
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The default cost for the OSPFv3 protocol running on the interface is obtained based on the rate of the port

Command mode

Interface configuration mode

Example

The following example shows how to set the cost for the OSPFv3 protocol running on interface vlan1 to 2:

interface vlan 1

ipv6 ospf cost 2

Related command

None

48.19 ipv6 ospf database-filter all out

Syntax

To designate an interface to filter those to-be-transmitted LSA, run the first one of the following two commands:

ipv6 ospf database-filter all out [**instance** *instance-id*]

no ipv6 ospf database-filter all out [**instance** *instance-id*]

Parameter

Parameter	Description
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The interface does not filter those to-be-transmitted LSAs

Command mode

Interface configuration mode

Example

The following example shows how to set interface vlan 1 to filter those to-be-transmitted LSAs:

interface vlan 1

ipv6 ospf database-filter all out

Related command

None

48.20 ipv6 ospf dead-interval

Syntax

To designate the dead interval of the neighboring router, run **ipv6 ospf dead-interval** ***seconds***. To resume the default value, run **ipv6 ospf dead-interval**

ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]

Parameter

Parameter	Description
seconds	Value of the dead interval for the neighboring router, which ranges from 1 to 2147483647 seconds
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The dead interval for the neighboring router is four times of hello-interval by default

Command mode

Interface configuration mode

Usage guidelines

The value of the **dead-interval** parameter will be written to the HELLO packet and will be transmitted along with the HELLO packet. It must be ensured that the **dead-interval** parameter must be identical with that between the neighboring routers and the value of the **dead-interval** parameter must be four times of the value of the **hello-interval** parameter

Example

The following example shows how to set the dead interval of the neighboring router on interface vlan1 to 60 seconds

interface vlan 1

ipv6 ospf dead-interval 60

Related command

None

48.21 ipv6 ospf hello-interval

Syntax

To designate the interval for transmitting the HELLO packet on the interface, run **ipv6 ospf hello-interval** ***seconds***. To resume the default settings, run **no ipv6 ospf hello-interval**

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

Parameter

Parameter	Description
seconds	Transmission interval of the HELLO packet, ranging from 1 to 65535 seconds
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The interval for the P2P or Broadcast interface to send Hello packets is 10 seconds, while the interval for the P2MP or NBMA interface to send Hello packets is 30 seconds

Command mode

Interface configuration mode

Usage guidelines

The value of the **dead-interval** parameter will be written to the HELLO packet and will be transmitted along with the HELLO packet. The smaller the hello-interval is, the sooner the change of the network topology will be found. However, much more path cost will be paid. It must be ensured that the parameter must be identical with that between the neighboring routers

Example

The following example shows that the interval for transmitting the HELLO packet on interface vlan1 is set to 20 seconds

interface vlan 1

ipv6 ospf hello-interval 20

Related command

ipv6 ospf dead-interval

48.22 ipv6 ospf mtu-ignore

Syntax

To set the MTU value of the transmitted DD packet to 0 on an interface and meanwhile omit the checkup of the MTU domain of the received DD packet, run the first one of the following two commands:

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter

Parameter	Description
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The value of the MTU domain of the DD packet is set to be the MTU value of this interface and MTU checkup is not omitted

Command mode

Interface configuration mode

Usage guidelines

OSPF judges whether the MTU value of the network segment, where an interface belongs, is consistent by checking the MTU value of the exchanged DD packet.If the MTU value of the received DD packet is bigger than the MTU value of this interface, the OSPF neighborhood cannot be set up

Example

The following example shows how to set interface vlan1 to omit MTU checkup.

interface vlan 1

ipv6 ospf mtu-ignore

Related command

None

48.23 ipv6 ospf neighbor

Syntax

To set the OSPF neighbor on the non-broadcast network interface, run the first one of the following two commands:

ipv6 ospf neighbor *router-id ipv6-address* [**cost** *number*] [**database-filter all out**] [**poll-interval** *seconds*] [**priority** *number*] [**instance** *instance-id*]

no ipv6 ospf neighbor *router-id ipv6-address* [**cost** *number*] [**database-filter all out**] [**poll-interval** *seconds*] [**priority** *number*] [**instance** *instance-id*]

Parameter

Parameter	Description
router-id	Means the router ID of a neighbor
ipv6-address	Means the local address of the neighbor's link
cost number	Means the neighbor's cost, whose value ranges from 1 to 65535
database-filter all out	Filters the transmitted LSAs
poll-interval seconds	Means the query interval of a neighbor
priority number	Means the neighbor's priority, whose value ranges from 0 to 255
instance instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

No neighbors are set

Command mode

Interface configuration mode

Usage guidelines

You shall specify a neighbor manually on the non-broadcast network. If neighbors invalidates, the Hello packet should be sent to this neighbor in poll interval

Example

The following example shows how to set the neighbor of interface vlan1

```
interface vlan 1
 ipv6 ospf neighbor 1.1.1.1 FE80::FEFA:F7FF:FE2E:2B63
```

Related command

None

48.24 ipv6 ospf network

Syntax

To set the network type for the interface, run the first one of the following two commands

ipv6 ospf network { **broadcast | non-broadcast | point_to_multipoint [broadcast | non-broadcast] | point-to-point**} [**instance** *instance-id*]

no ip ospf network { **broadcast | nonbroadcast | point_to_multipoint [broadcast | non-broadcast] | point-to-point**} [**instance** *instance-id*]

Parameter

Parameter	Description
broadcast	Sets the network type of the interface to **broadcast**
nonbroadcast	Sets the network type of the interface to **NBMA**
point-to-multipoint	Sets the network type of the interface to **point-to-multipoint**
point-to-point	Sets the network type of the interface to **point-to-point**
instance instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Command mode

Interface configuration mode

Usage guidelines

The interface in the broadcast network without multi-address access should be set to NBMA. In the NBMA network, the network should be set to **point-to-multipoint** if any two routers cannot be ensured to be directly reachable

Example

The following example shows how to set interface vlan1 to NBMA.

interface vlan 1

ipv6 ospf network non-broadcast

Related command

None

48.25 ipv6 ospf priority

Syntax

To configure the priority for the interface to choose the router, run **ipv6 ospf priority** ***priority.*** To resume the default value, run **no ipv6 ospf priority**

ipv6 ospf priority *priority* [**instance** *instance-id*]

no ipv6 ospf priority *priority* [**instance** *instance-id*]

Parameter

Parameter	Description
priority	Priority to choose the router, ranging between 0 and 255
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The default priority for the interface to choose the routers is 1

Command mode

Interface configuration mode

Usage guidelines

When two routers in the same network segment want to be the selection router, the router with higher priority will be selected. If the priority of the two routers is the same, the router with a larger ID is selected. When the priority of a router is 0, the router cannot be selected as the designated router or the standby designated router. The priority is effective only on the networks except the nonpoint-to-point network

Example

The following example shows how to set the priority to 8 when interface vlan1 selects the selection router

interface vlan 1

ipv6 ospf priority 8

Related command

None

48.26 ipv6 ospf retransmit-interval

Syntax

To designate the retransmission interval for transmitting LSA between the interface and the neighboring router, run **ipv6 ospf retransmit-interval seconds**. To resume the default value, run **no ipv6 ospf retransmit-interval**

ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

Parameter

Parameter	Description
seconds	Transmission interval for transmitting the link state broadcast between the interface and the neighboring router, ranging between 1 and 3600 seconds
instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The default interval for transmitting the link state broadcast between the interface and the neighboring router is 5 seconds

Command mode

Interface configuration mode

Usage guidelines

When a router transmits the link-state broadcast to its neighbor, the command will maintain the link-state broadcast until the peer receives the acknowledgement. If the link-state broadcast is not received during the transmission interval, it will be retransmitted. The value of the **seconds** parameter must be larger than the round-trip time for a packet transmitting between two routers

Example

The following example shows how the default interval for transmitting the link-state broadcast between interface vlan1 and the neighboring router is set to 8 seconds

interface vlan 1

ipv6 ospf retransmit-interval 8

Related command

None

48.27 ipv6 ospf transmit-delay

Syntax

To set the delay for the link-state broadcast to be transmitted on the interface, run **ipv6 ospf transit-delay time**. To resume the default value, run **no ipv6 ospf transit-delay**

ipv6 ospf transmit-delay *time* [**instance** *instance-id*]

no ipv6 ospf transmit-delay *time* [**instance** *instance-id*]

Parameter

Parameter	Description
time	Means the delay of link state broadcast transmission on an interface, which ranges from 1 to 3600 seconds

instance-id	Specifies the OSPF instance ID of the interface, whose default value is 0

Default value

The default delay for the link-state broadcast to be transmitted on the interface is 1 second

Command mode

Interface configuration mode

Example

The following example shows how to set the delay for transmitting the link-state broadcast on interface vlan1 to 3 seconds

interface vlan 1

Ipv6 ospf transmit-delay 3

Related command

None

48.28 passive-interface

Syntax

To forbid a designated interface to transmit or receive the OSPFv3 packets, run the first one of the following two commands:

passive-interface { *interface-type* *interface-number* | all }

no passive -interface { *interface-type* *interface-number* | all }

Parameter

Parameter	Description
interface-type *interface-number*	Means the interface type and the interface ID
all	Means all interfaces

Default value

The interface is allowed to transmit or receive the OSPFv3 packets

Command mode

Routing configuration mode

Usage guidelines

Different processes can forbid a same interface to transmit or receive the OSPFv3 packets, but the passive-interface command takes effect only on the OSPFv3 interface

Example

The following example shows how to forbid interface vlan1 to receive and transmit the OSPFv3 packets in the OSPFv3 process

router ospfv3 100

passive-interface vlan 1

Related command

None

48.29 redistribute

Syntax

To configure the route where OSPF forwards other routing protocols, run **redistribute**. To resume the default settings, run **no redistribute**.

redistribute protocol [*as-number*] [**route-map** map-tag]

no redistribute protocol [*as-number*] [**route-map**]

Parameter

Parameter	Description
protocol	Means to forward the learned original protocol.
as_number	Means the number of the autonomous system which is not for the **connect** or **static** parameter
map-tag	Means the name of the route map

Default value

Not forward

Command mode

Routing configuration mode

Usage guidelines

None

Example

The following example shows how to forward the static route in OSPF process 1:

interface vlan 1

ipv6 ospf 1 area 0

!

router ospfv3 1

router-id 2.2.2.2

redistribute static

48.30 router ospfv3

Syntax

To enable OSPFv3 and enter the OSPFv3 configuration view, run the first one of the following two commands:

router ospfv3 *process-id*

no router ospfv3 *process-id*

Parameter

Parameter	Description
process-id	Identifies the OSPF process. It is a positive integer distributed by the local router

Default value

None

Command mode

Global configuration mode

Usage guidelines

One router may have multiple OSPFv3 processes

Example

The following example shows how to set an OSPFv3 process, whose process ID is 109:

router ospfv3 109

Related command

ipv6 ospf area

48.31 router-id

Syntax

To set the router ID in the autonomous system for the router on which the OSPFv3 protocol is running, run the first one of the following two commands:

router-id *router-id*

no router-id *router-id*

Parameter

Parameter	Description
router-id	Means the identifier of the router, which is in the IPv4 address format

Default value

If an IPv4 address has already configured on a router before OSPFv3 is enabled, the router will automatically choose an IPv4 address as its ID

Command mode

Routing configuration mode

Usage guidelines

The router ID is the unique identifier of a OSPFv3-running router in the autonomous system, so the router IDs of two routers in the autonomous system are different. If a router has no router ID, the OSPFv3 process cannot go on

Example

The following example shows how to set the router ID of OSPFv3 process 1 to 2.2.2.2:

router ospfv3 1

router-id 2.2.2.2

48.32 show ipv6 ospf

Syntax

To display the main OSPFv3 information, run the following command:

show ipv6 ospf [*process-id*]

Parameter

Parameter	Description
process-id	Means the OSPF process ID

Default value

None

Command mode

EXEC

Usage guidelines

The information exported by the command can help checking the OSPFv3 faults. If the **process-id** parameter follows the command, the information about the global configuration of the OSPFv3 process is displayed

Example

The following example shows that the configuration information about all OSPFv3 processes will be displayed

```
Switch#show ipv6 ospf 1
 Routing Process "OSPFv3 (1)" with ID 1.1.1.1, 0x7266520
 SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 LSDB age interval 60 secs
 Number of external LSA 0. (0x4d5d4e0). Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 7
 Number of LSA received 15
 Number of areas in this router is 2
 Number of transit areas in this router is 0
    Area BACKBONE(0), 0x71b7730
        Number of interfaces in this area is 1
        SPF algorithm executed 4 times
        Number of LSA 6. (0x4d5cfe0). Checksum Sum 0x40FB3
        Number of Unknown LSA 0
    Area 0.0.0.1, 0x71b6de8
        Number of interfaces in this area is 1
        SPF algorithm executed 1 times
        Number of LSA 3. (0x4d59278). Checksum Sum 0x191B6
        Number of Unknown LSA 0
```

Relative fields are explained in the following table:

Domain	Description
Routing Process "OSPFv3 1"	ID of the process

with ID 1.1.1.1	ID of the router
SPF schedule delay 5 secs, Hold time between SPFs 10 secs	Two timer values relative with OSPF
Number of areas in this router is 2	Number of the currently-configured fields, and parameters configured in each field
Number of LSA originated / received 7 /15	The number of received and generated quantity of LSAs is 7, 15 respectively
Number of external LSA 0	Number of fifth type lsa in the database
SPF algorithm executed 4 times	SPF algorithm execution statistics

48.33 show ipv6 ospf database

Syntax

To display the database information about the OSPFv3 connection state, run the following command:

show ipv6 ospf database [router | network | inter-prefix | inter-router | external | nssa | link | intra-prefix][adv-router router-id][database-summary]

Parameter

Parameter	Description
router	Means the LSA type is the router
network	Means the LSA type is the network
inter-prefix	Means the LSA type is the inter-domain route
inter-router	Means the LSA type is the inter-domain router
external	Means the LSA type is the exterior route
nssa	Means the LSA type is the nssa exterior route
link	Means the LSA type is the link
intra-prefix	Means the LSA type is the inside-domain route
adv-router	Means to declare the router ID
database-summary	Means to show database summary

Default value

None

Command mode

EXEC

Usage guidelines

The information exported by the command can help to check the database information about the OSPFv3 connection state and to find the reason of the faults

Example

```
Switch#show ipv6 ospf data

            OSPFv3 Router with ID (1.1.1.1) (Process 1)


                Link-LSA (Interface VLAN1)

Link State ID    ADV Router      Age Seq#       CkSum  Prefix
0.0.0.26         1.1.1.1         396 0x80000001 0x6517    1
0.0.0.3          5.6.2.1         442 0x80000001 0xf2cb    1
0.0.0.6          11.1.1.1        433 0x80000001 0x4146    1

                Router-LSA (Area 0.0.0.0)

Link State ID    ADV Router      Age Seq#       CkSum  Link
0.0.0.0          1.1.1.1         320 0x80000004 0x30b8    1
0.0.0.0          5.6.2.1          21 0x80000006 0x985a    1
0.0.0.0          11.1.1.1        388 0x80000004 0xb93a    1

                Network-LSA (Area 0.0.0.0)

Link State ID    ADV Router      Age Seq#       CkSum
0.0.0.6          11.1.1.1        389 0x80000002 0xfbf3

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID    ADV Router      Age Seq#       CkSum
0.0.0.1          1.1.1.1         315 0x80000002 0xe69c
```

Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix	Reference
0.0.0.2	11.1.1.1	387	0x80000001	0xaed1	1	Network-LSA

……

Relative fields are explained in the following table:

Domain	Description
Area 0.0.0.0	Current area
Link-LSA	LSA type
Link State ID	LSA ID
ADV Router	Releases the router
Age	Releases the age
Seq #	Generates the sequence ID
Checksum	Means the checksum

48.34 show ipv6 ospf interface

Syntax

To display the information about the OSPFv3 interface, run the following command:

show ipv6 ospf interface [type] [index]

Parameter

Parameter	Description
type	Port type
index	Port number

Default value

None

Command mode

EXEC

Usage guidelines

According to the information displayed by the command, you can check the OSPFv3 configuration and its running state, which helps you to detect the OSPFv3 faults

Example

```
Switch# show ipv6 ospf interface
VLAN1 is up, line protocol is up
  Interface ID 26,    Interface MTU 1500
  Interface bandwidth 1000000
  IPv6 Prefixes
    2001::1/64
    fe80::fefa:f7ff:fe2e:2b63/64 (Link-Local Address)
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0, 0x71b7520
    Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DROther, Priority 1
    Designated Router (ID) 11.1.1.1
      Interface Address fe80::fefa:f7ff:fe81:139
    Backup Designated Router (ID) 5.6.2.1
      Interface Address fe80::2e0:fff:fe87:0
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:04
    Neighbor Count is 2, Adjacent neighbor count is 2
    Number of LSA 3. (0x4d5c7e8). Checksum Sum 0x19928
    Number of Unknown LSA 0
……
Switch#
```

Relative fields are explained in the following table:

Domain	Description
Link-Local Address	Address of port **IPv6 link-local**

Nettype	Network type of the OSPF interface
OSPFv3 Process (1)	ID of the OSPF process
Area 0.0.0.0	Current backbone domain
Router ID	ID of the router where the process belongs
Cost	Cost of the OSPF interface of the router
Transmit Delay is	Transmission delay
Priority	Priority for the interface of the router
Hello interval	Transmission interval of the Hello packet
Dead timer	Dead time
Retransmit	Retransmission interval
State	State of the OSPF port
Designated Router (ID)	ID of the designated router and the IP address of its port
Backup Designated Router (ID)	ID of the backup designated router and the IP address of its port
Neighbor Count is	Number of the neighboring routers
Adjacent neighbor count is	Number of neighbors that have established the neighborhood relation

48.35 show ipv6 ospf neighbor

Syntax

To display the information about OSPFv3 neighbor, run the following command

show ipv6 ospf neighbor [*interface_type interface_number*| *router-id*| *detail*]

Parameter

Parameter	Description
interface_type	Port type
interface_number	Port number
router-id	Router ID
detail	Displays the detailed information.

Default value

None

Command mode

EXEC

Usage guidelines

The information displayed by the command can help you to check whether the OSPFv3 neighbor configuration is right and to detect the OSPFv3 faults

Example

```
Switch#show ipv6 ospf neighbor

OSPFv3 Process (1)

Neighbor ID     Pri   State           Dead Time   Interface    Instance ID

5.6.2.1           1   Full/Backup     00:00:31    VLAN1        0

11.1.1.1          1   Full/DR         00:00:32    VLAN1        0

Switch#
```

Relative fields are explained in the following table:

Domain	Description
OSPFv3 process	ID of the OSPF process
Neighbor	ID of a neighbor
Pri	Priority of a neighbor
State	Connection state related with the neighbor
DeadTime	Time of neighbor invalidation
Interface	Interface used by a router to reach its neighbor
Instance ID	Instance ID number

48.36 show ipv6 ospf route

Syntax

To display the information about the OSPFv3 routing table, run the following command:

show ipv6 ospf route

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The information displayed by the command can help you browse the OSPFv3 routing table and confirm whether the OSPFv3 trouble diagnosis is correctly carried out

Example

```
Switch#show ipv6 ospf route

OSPFv3 Process (1)

    Destination                                 Metric

        Next-hop

C   23::1/128                                   1

        directly connected, Loopback9

IA  52::1/128                                   2

        via fe80::fefa:f7ff:fe81:139, VLAN1

E2  99::1/128                                   1/150

        via fe80::2e0:fff:fe87:0, VLAN1

C   2001::/64                                   1

        directly connected, VLAN1

Switch#
```

Relative fields are explained in the following table:

Domain	Description
Destination	Destination network segment
Metric	Cost of a route
Next-hop	Address of the next hop

48.37 show ipv6 ospf virtual-link

Syntax

To display the information about the OSPFv3 virtual link, run the following command:

show ipv6 ospf virtual-link

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

According to the information exported by the command, you can check the state of the OSPFv3 virtual link

You can run **show ipv6 ospf neighbor** to check the detailed information about the adjacent neighbor

Example

```
Switch #show ipv6 ospf virtual-link
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface eth0, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

Relative fields are explained in the following table:

Domain	Description
neibhbor ID	Neighbor ID of the peer
neighbor state	Neighborhood state for the neighbor
TransArea	Transmission area
cost	Minimum cost for reaching the peer in the transmission area If the value of the cost is 0, it means that the peer is unreachable
Hello Interval	Current transmission interval for the Hello packet
DeadTime	Time of neighbor invalidation
Retrans	Retransmission interval
Adjacency state	State of the virtual link interface

Related command

area vritual-link

show ipv6 ospf neighbor

48.38 summary-prefix

Syntax

To configure the address for OSPFv3 to create the route aggregation, run **summary-prefix**. To cancel the address of route aggregation, run **no summary-prefix**

summary-prefix *ipv6-prefix /prefix-length [not-advertise]*

no summary-prefix *ipv6-prefix /prefix-length [not-advertise]*

Parameter

Parameter	Description
ipv6-prefix	Aggregation address with the designated address range
prefix-length	Subnet mask of the aggregation route
not-advertise	*Do not post*

Default value

None

Command mode

Routing configuration mode

Usage guidelines

Multiple groups of addresses are summarized. Routes learned from other routing protocols can also be summarized. After the aggregation, all covered networks cannot be transmitted to other routing fields. The cost of the summary route is the minimum value among the cost values of all summary routes. The command cannot be used to reduce the size of the routing table

The command is used by OSPFv3 to enable the ASBR to notify an external route of being an aggregation route to replace all external routes. The command is only used to aggregate the OSPFv3 routes of other routing protocols. You can run **area range** in OSPFv3 to summarize the routes

Example

In the following example, the summary address 2001::/64 stands for addresses such as 2001::/80, 2001::1/64 and so on, and only address 2001::/64 is broadcasted

summary-prefix 2001::/64

Related command

area range

48.39 timers delay

Syntax

To designate a delay interval between OSPF receiving a topology change and starting a shortest path priority calculation, run **timers delay** ***spf-delay***. To resume the default settings, run **no timers delay**

timers delay *spf-delay*

no timers delay *spf-delay*

Parameter

Parameter	Description
spf-delay	Delay between the topology change and calculation start, ranges from 0 to 65535. Its default value is 5 seconds. If the value is 0, there is no delay. That is, the calculation will be promptly started if changes occur

Default value

spf-delay: 5 seconds

Command mode

Routing configuration mode

Usage guidelines

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time

Example

The following example shows how to set the time for OSPF to start calculating the delay is 10 seconds.

timers delay 10

48.40 timers hold

Syntax

To set the interval between two continuous SPF calculations, run **timers hold**. To resume the default settings, run **no timers hold**

timers hold *spf-holdtime*

no timers hold *spf-holdtime*

Parameter

Parameter	Description
spf-holdtime	Minimum value between two continuous calculations It ranges between 0 to 65535 seconds. Its default value is 10 seconds; when it is 0, there is no interval between the two continuous calculations

Default value

spf-holdtime: 10 seconds

Command mode

Routing configuration mode

Usage guidelines

The smaller value the delay is set to, the faster the network change is reflected. However, it will take the processor more time

Example

The following example shows how to set the interval between two successive SPF calculations to 20 seconds:

timers hold 20

48.41 timers age

Syntax

To configure the time interval of OSPF checking LSA database aging, run the following command. To return to the default setting, use the no form of this command

timers age *agetime*

no timers age *agetime*

Parameter

Parameter	Description
agetime	Check LSDB database every agetime second and delete aging lsa

Default value

agetime: 60 seconds

Command mode

Routing configuration mode

Usage guidelines

The smaller the time interval, the faster the database reflects but with more time for the processor

Example

The following example shows how to set the aging time of OSPF checking LSDB to 50 seconds

timers age 50

Chapter 49 PDP Configuration Commands

49.1 pdp timer

Syntax

[no|default] pdp timer seconds

It is used to set the time of the PDP timer

Parameter

Parameter	Description
seconds	Means the interval for PDP to transmit packets outside, which ranges from 5 seconds to 254 seconds

Default

The default settings is 60 seconds

Usage Guidelines

This command is configured in global configuration mode

Example

The following example shows that a switch transmits PDP packets every 5 seconds

pdp timer 5

49.2 pdp holdtime

Syntax

[no|default] pdp holdtime seconds

It is used to set the PDP holdtime

Parameter

Parameter	Description
seconds	Means the time needed for deleting the neighbor information, which ranges from 10 to 255 seconds

Default

The default settings is 180 seconds

Usage Guidelines

This command is configured in global configuration mode

Example

The following example shows that the neighbor information is kept for 15 seconds

pdp holdtime 15

49.3 pdp version

Syntax

[no] pdp version <1|2>

It is used to set the PDP version

Parameter

Parameter	Description
version	Means the PDP version, which is 1 or 2

Default

The default version is version 2

Usage Guidelines

This command is configured in global configuration mode

Example

The following example shows that the PDP version of a switch is version 1

pdp version 1

49.4 pdp run

Syntax

[no] pdp run

It is used to enable PDP

Parameter

None

Default

The PDP protocol is disabled

Usage Guidelines

This command is configured in global configuration mode

Example

The following example shows to disable PDP

no pdp run

49.5 pdp enable

Syntax

[no] pdp enable

It is used to enable or disable PDP on a port

Parameter

None

Default

PDP is enabled by default

Usage Guidelines

This command is set in port configuration mode and takes effect in port or global mode only when PDP is enabled

Example

The following example shows that PDP is disabled on port g0/1

switch_config_g0/1#no pdp enable

49.6 show pdp traffic

Syntax

show pdp traffic

It is used to display the number of received PDP packets

Parameter

None

Default

None

Usage Guidelines

It is used to browse the running of PDP

Example

Switch_config#show pdp traffic

Packets output: 253491, Input: 0

Hdr syntax: 0, Chksum error: 0

No memory: 0, Invalid packet: 0

49.7 show pdp neighbor

Syntax

show pdp neighbor

It is used to display the PDP neighbor

Parameter

None

Default

None

Usage Guidelines

It is used to browse the running of PDP neighbor

Example

Switch_config#show pdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Gig0/1	169	Gig0/1	BDCOM, RISC	R S

Chapter 50 Port Additional Characteristics Configuration Commands

50.1 Configuring Port Isolation

50.1.1 port-protected

Syntax

[no] port-protected group-id

Configure a port isolation group with the above command

Parameter

Parameter	Description
group-id	Configure a port isolation group 1-28

Default

None

Usage Guidelines

Configure the command in global configuration mode for the group-based isolation

Example

Configure the port isolation group 1

Switch_config#port-protected 1

50.1.2 description

Syntax

description word

Configure description of the port isolation group with the above command

no description

Delete description with the above command

Parameter

Parameter	Description

Word	Configure description of the port isolation group, no more than 31 characters

Default

None

Usage Guidelines

Configure the command in global configuration mode for the description

Example

The following example shows how to configure description g1 of the port isolation group 1

Switch-config-p1#description g1

50.1.3 switchport protected

Syntax

switchport protected *<group-id>*

no switchport protected

Configure the port isolation with the above command

Parameter

Parameter	Description
group-id	Choose the port isolation 1-28

Default

None

Usage Guidelines

The command works in the layer-2 interface. The default command is based on the non-group isolation that does not need to configure group-id in the end. If the command is based on group-based isolation, all ports need to configure group-based isolation in global configuration mode. Only after deleting isolations in all ports, the isolation type can be configure again

Example

The following example shows how to configure the non-group based isolation on interface g0/1

Switch_config_g0/1#switchport protected

50.2 Configuring Storm-control

50.2.1 storm-control

Syntax

storm-control { **broadcast** | **multicast** | **unicast** } **threshold** *count*

no storm-control { **broadcast** | **multicast** | **unicast** } **threshold**

Configure the port storm control with the above command

Parameter

Parameter	Description
broadcast	Specifies storm control for broadcasting
multicast	Specifies storm control for multicast
unicast	Specifies storm control for unknown unicasts
count	Defines the traffic threshold for storm occurrence

Default

No storm control function

Usage Guidelines

The command works in the layer-2 interface mode

Example

The following example shows how to configure unknown unicast frame storm 20PPS allowed on g0/1

Switch_config#interface g0/1

Switch_config_g0/1#storm-control unicast threshold 20

50.2.2 storm-control mode

Syntax

storm-control mode { kbps | pps }

no storm-control mode

Configure the unit of port storm control threshold with the above command

Parameter

Parameter	Description
kbps	Sets the storm threshold in kbps, with a minimum unit of 64kpbs
pps	Sets the storm threshold in pps, with a minimum unit of 1 pps

Default

Unit: pps.

Usage Guidelines

The command works in layer-2 port configuration mode

Ensure that there are no configured storm control functions during configuration

Example

The following example shows how to set the unit of storm control to kbps on port g0/1

Switch_config#interface g0/1

Switch_config_g0/1#storm-control mode kbps

50.2.3 storm-control action

Syntax

storm-control {broadcast | multicast} action {shutdown | block | resume}

no storm-control {broadcast | multicast} action

Configure the storm control action function of the port

Parameter

Parameter	Description
shutdown	When the port traffic reaches the threshold, the port will close
block	When the port traffic reaches the threshold, the port will block
resume	Restore ports that have been closed or blocked due to storm control

Default

Disable storm control action

Usage Guidelines

The command works in the layer-2 interface mode

When the **storage control auto resume** is not configured, the port status will not be automatically restored, and manual configuration of the **storage control action resume** is required to enable the port packet forwarding

Only in broadcasting and multicast modes based on PPS, storm control action operations are supported, and the corresponding storm threshold needs to be configured before configuration

Example

The following example shows how to set the action of broadcasting storm control on g0/1 to shutdown

Switch_config#interface g0/1

Switch_config_g0/1#storm-control mode pps

Switch_config_g0/1#storm-control broadcast threshold 20

Switch_config_g0/1#storm-control broadcast action shutdown

50.2.4 storm-control auto-resume

Syntax

storm-control {broadcast | multicast} auto-resume [*second* **]**

no storm-control {broadcast | multicast} auto-resume

Configure the storm control function of the port

Parameter

Parameter	Description
second	The time, in seconds, that the port automatically recovers. It defaults to 60 seconds

Default

The storm control function is not enabled

Usage Guidelines

This command works in layer-2 port configuration mode

Only in broadcasting and multicast modes based on PPS, storm-control auto-resume is supported, and the corresponding **storm-control action** needs to be configured before configuration

Example

The following example shows how to set the automatic recovery time for broadcast storm control on g0/1 to 100 seconds.

Switch_config#interface g0/1

Switch_config_g0/1#storm-control mode pps

Switch_config_g0/1#storm-control broadcast threshold 20

Switch_config_g0/1#storm-control broadcast action shutdown

Switch_config_g0/1#storm-control broadcast auto-resume 100

50.2.5 storm-control notify

Syntax

storm-control notify { log | trap }

no storm-control notify { log | trap }

Configure the storm control reporting alarm function of the port

Parameter

Parameter	Description
log	Reports an alarm on the syslog printing method
trap	Reports the alarm through snmp rap

Default

Disable the storm control reporting alarm function

Usage Guidelines

This command works in layer-2 port configuration mode

Two methods can be enabled simultaneously

Example

The following example shows how to set storm control alarm through the syslog on g0/1

Switch_config#interface g0/1

Switch_config_g0/1#storm-control notify log

50.3 Configuring Switchport Rate-limit

Syntax

switchport rate-limit {*band* | ***bandwidth*** *percent*} { **ingress**|**egress**}

no switchport rate-limit{ ingress|egress}

Configure the flow rate limitation for the port

Parameter

Parameter	Description
Band	Flow rate. 64kbps-step rate limitation on a port
percent	Flow rate ratio, unit: 1%
ingress	Functions at the ingress port
egress	Functions at the egress port

Default

The port has no port rate limitation

Usage Guidelines

This command works in layer-2 port configuration mode

Example

Set the incoming flow rate limitation on interface g0/1 to 1Mbps

Switch_config#interface g0/1

Switch_config_g0/1#switchport rate-limit 16 ingress

50.4 Configuring Port Loop Check

Syntax

[**no**] **keepalive** *second*

To configure the interval for a port to transmit the loop check packets, run **keep alive** command

Parameter

Parameter	Description
Second	Time interval. Unit: second

Default

The time interval is 12 seconds by default

Usage Guidelines

Configure in the physical port configuration mode

Example

The following example shows how to set the transmission interval on interface g0/1 to 10 seconds

Switch_config#interface g0/1

Switch_config_g0/1#keepalive 10

50.5 Configuring Port MAC-address learning

Syntax

[**no**] **switchport disable-learning**

Configure the learning MAC address on the port

Parameter

None

Default

Enable the learning MAC address on the port

Usage guidelines

Configure in the physical port configuration mode

Example

The following example shows how to disable MAC address learning on the interface g0/1

Switch_config#interface g0/1

Switch_config_g0/1#switchport disable-learning

50.6 Configuring Port Security

50.6.1 switchport port-security mode

Syntax

switchport port-security mode {**dynamic | static** *accept/reject* **| sticky**}

[**no**] **switchport port-security mode**

Set the static mode of the security port

Parameter

None

Default

The port security function is not enabled

Usage guidelines

Configure the command on the physical port configuration mode

Example

The following example shows how to configure interface g0/1 in the dynamic interface security mode

Switch_config#inter g0/1

Switch_config_g0/1#switchport port-security mode dynamic

50.6.2 switchport port-security dynamic

Syntax

switchport port-security dynamic maximum *dynamic_number*

[**no**] **switchport port-security dynamic maximum**

To configure the maximum number of MAC addresses when the port is in dynamic security mode, run **switchport port-security dynamic maximum** command

Parameter

Parameter	Description	Value ranges
dynamic_number	Means the maximum number of MAC addresses	1-2048

Default

The number of MAC addresses that can be learned is 1

Usage guidelines

Configure the command on the physical port configuration mode

Example

The following example shows how to apply maximum MAC addresses on interface g0/1 and set the learnable MAC address to 10

Switch_config#inter g0/1

Switch_config_g0/1# switchport port-security dynamic maximum 10

50.6.3 switchport port-security static mac-address

Syntax

[**no**] **switchport port-security static mac-address H.H.H**

Configure the static MAC address of the security port

Parameter

None

Default

None

Usage Guidelines

Configure the command on the physical port configuration mode

Example

The following example shows how to configure mac: 0001.0002.0003 to static security mac

Switch_config#inter g0/1

Switch_config_g0/1# switchport port-security static mac-address 1.2.3

50.6.4 switchport port-security sticky

Syntax

Switchport port-security sticky {maximum *sticky_number***| mac-address** H.H.H**| aging-time** *aging_time***}**

[no] switchport port-security sticky {maximum | mac-address H.H.H| aging-time }

Configure the port-security sticky of MAC address

Parameter

Parameter	Description
sticky_number	The maximum number of addresses that can be learned on the port. Default is 100, range: 1-2048
H.H.H	Mac address
aging_time	Aging time. Unit: minutes. The default is 0, the range: 0-100

Default

The port sticky of MAC address is not enabled

Usage Guidelines

Configure the command on the physical port configuration mode

Example

The following example shows how to manually configure mac: 4433.0002.0021 to security sticky mac address

Switch_config#inter g0/1

Switch_config_g0/1# switchport port-security sticky mac-address 4433.0002.0021

50.7 Configuring Port Binding

Syntax

switchport port-security bind|block {**ip|arp|both-arp-ip** *ip-addr*| **mac** *mac-addr*}

no switchport port-security bind|block {**ip|arp| both-arp-ip** *ip-addr* **mac** *mac-addr*}

To bind a MAC address to an IP address, run the first one of the above commands

To cancel the address binding one by one or to exit the port binding state by cancelling all addresses on the port, run the no form of the command

Parameter

Parameter	Description	Value ranges
ip-addr	IP address	A.B.C.D
Mac-addr	Mac address	H.H.H

Default

None

Description

This command works in layer-2 port configuration mode

The port binding function is forbidden by default. However, if one address is bound, the port is then in binding state unless you use the negative form of this command to clear all bound address items

Example

The following example shows how to bind IP address 1.2.3.4 to MAC address 0001.0001.1111 on interface g0/1 to decline the IP packets and ARP packets from the bound address

Switch_config#inter g0/1

Switch_config_g0/1# switchport port-security block both-arp-ip 1.2.3.4 mac 0001.0001.1111

50.8 Configuring SVL/IVL

Syntax

[no]vlan shared-learning

The command is used to configure share vlan learning (SVL)

Parameter

None

Default

Configure Independent Vlan Learning (IVL) on the port

Usage Guidelines

Configure the command in global configuration mode

Example

The following example shows how to configure shared learning.、

Switch_config#vlan shared-learning

50.9 Configuring Link Scan

Syntax

[no] Link scan [normal | fast] *interval*

To set the scan interval of an interface, run the above command

Parameter

Parameter	Description
[normal | fast]	Normal: standard link scan mode Fas: fast link scan mode
interval	Scan interval, unit: 1ms, 10-1000

Default

The default scan interval in the standard mode is 500ms

The default scan interval in the fast mode is 10ms

Usage Guidelines

Configure the command in global configuration mode. The Fast mode is mainly used for collaborating with the protocol, such as RSTP. Discover the interface up/down in the normal mode

Example

The following example shows how to set the scan interval of a switch to 20ms

Link scan normal 20

50.10 Configuring Port Enhanced Link Status Check

Syntax

[no] switchport enhanced-link

To enable/disable status check of the port enhanced link, run the above command

Parameter

None

Default

Disable status check of the port enhanced link

Usage Guidelines

Configure the command in port configuration mode

Example

The following example shows how to enable status check of the port g0/1 enhanced link

Switch_config#interface g0/1

Switch_config_g0/1#switchport enhanced-link

50.11 Configuring System mtu

Syntax

[no] system mtu *mtu*

The command is used to configure mtu

Parameter

Parameter	Description
mtu	Configures system mtu, the value ranges from 1500 to 9216

Default

The default mtu is 1500 bytes

Usage Guidelines

Configure the command in the global configuration mode

Example

The following example shows how to configure mtu to 2000 bytes

Switch#config

Switch_config#system mtu 2000

Chapter 51 Configuring Port Mirroring Commands

51.1 mirror

Syntax

[**no**] **mirror session** *session_number* {**destination** {**interface** *interface-id* } { **rspan** *vid tpid*} | **source** {**interface** *interface-id* [, | -] [**rx** | **tx** | **both**] }

The command is used to configure port mirroring

Parameters

Parameter	Description
session_number	Number of port mirroring, whose value ranges from 1 to 4
destination	Information about the destination port mirroring
vid	Vid of remote mirror tag
tpid	Tpid of remote mirror tag
source	Information about the mirrored port
rx / *tx* /*both*	Data flow that will be mirrored **rx** means that the input data is mirrored. **tx** means that the output data is mirrored. **both** means that input and output data are mirrored

Default

None

Usage Guidelines

Configure the command in the global configuration mode

Note:

When the unknown unicasts, broadcast and other unknown unicast output the mirrored data, configure mirror session 1 as a source port

Example

Local mirror: The following example shows how to configure interface g0/2 to the output mirror of interface g0/1

Switch_config# mirror session 1 destination interface g0/2

Switch_config# mirror session 1 source interface g0/1

Remote mirror: The following example shows how to configure interface g0/2 to the local output mirror

port of interface g0/1. The remote mirror vlan is 100, and the tpid is 0x8100

Switch_config# mirror session 1 destination interface g0/2 rspan 100 0x8100

Switch_config# mirror session 1 source interface g0/1

51.2 show mirror

Syntax

show mirror [session *session_number]*

It is used to display the port mirroring information

Parameter

Parameter	Description
session_number	Number of port mirroring, value range from 1 to 4

Default

None

Usage Guidelines

It is used to display the port mirroring information

Example

The following example shows how to display the port mirroring information of the session 1

Switch_config#show mirror session 1

Session 1

Destination Ports: g0/3

Source Ports:

RX Only: None

TX Only: None

Both: g0/2

Chapter 52 Power Over Ethernet Configuration Commands

52.1 POE Configuration Commands

52.1.1 show poe system

Syntax

It is used to display the information about POE-related systems

show poe system

Parameter

None

Default

None

Command Mode

Monitoring mode

Usage Guidelines

POE DRIVER: means the drive of the chip

POE CHIP: means the detailed chip type

POE Port Num: means the maximum POE ports

PSE PowerManagement: means the power source management mode (automatic, preempt, non-preempt)

PSE Total Power: Total power of the power source equipment

PSE Usage Threshold: power alarm (it is set according to the percentage)

PSE Alarm Power: means the power alarm threshold

PSE Lower-Port-Disable Power: The threshold of the power supply for the relatively high priority preempt, which is effective only in non-automatic mode

PSE Lower-Port-NoConnect Power: The threshold of the power supply to forbid the lower or same-level priority preempt, which is effective only in non-automatic mode

PSE Consumed Power: the used power consumption

PSE Peak Power: peak power of the power source equipment, which is effective when the power statistics is enabled

PSE Mib Notification: MIB notification occurs when the power supply for a port changes or the power changes

PSE Temperature PSE: temperature of the chip

Example

Switch#show poe system

POE DRIVER:PETH PD69012 DRV

POE CHIP:PD69012

POE Port Num:24

PSE PowerManagement:Preemptive

PSE Total Power:80000 mW

PSE Usage Threshold:80%

PSE Alarm Power:64000 mW

PSE Lower-Port-Disable Power:62000 mW

PSE Lower-Port-NoConnect Power:44000 mW

PSE Consumed Power:47500 mW

PSE Peak Power:101300 mW

PSE Mib Notification:Disable

PSE Temperature:38 degree

Related Command

None

52.1.2 show poe all

Syntax

Displays the information description table of the POE port

show poe all

Parameter

None

Default

None

Command Mode

Monitoring mode

Usage Guidelines

Port enabled/disabled: To enable or disable power supply for a port

Port Detection: means the power supply state of a port, which may be disabled, searching, delivering-power, fault and so on. Delivering-power: means the power supply is normal

Port pairs: the ordering of the power line of a port, of which **signal** means the power supply by way of the signal line and **spare** that by way of the spare line

Port priority: means the priority for port's power supply and it from high to low is critical, high and low

Example

Switch#show poe all

Port	Enable	Status	Pair	Priority
f0/3	enabled	disabled	signal	low
f0/4	enabled	disabled	signal	low
f0/2	enabled	disabled	signal	low
f0/1	enabled	disabled	signal	low
f0/5	enabled	disabled	signal	low
f0/6	enabled	disabled	signal	low
f0/7	enabled	disabled	signal	low
f0/8	enabled	disabled	signal	low
f0/9	enabled	searching	signal	high
f0/10	enabled	searching	signal	high
f0/11	enabled	searching	signal	high
f0/12	enabled	searching	signal	high
f0/13	enabled	delivering-power	signal	high
f0/14	enabled	searching	signal	high
f0/15	enabled	delivering-power	signal	high
f0/16	enabled	searching	signal	high
f0/17	enabled	disabled	signal	low
f0/18	enabled	disabled	signal	low
f0/19	enabled	disabled	signal	low
f0/20	enabled	disabled	signal	low
f0/21	enabled	disabled	signal	low
f0/22	enabled	delivering-power	signal	low
f0/23	enabled	delivering-power	signal	low
f0/24	enabled	delivering-power	signal	critical

Related Command

None

52.1.3 show poe power

Syntax

It is used to display the information about the power supply of all ports

show poe power

Parameter

None

Default

None

Command Mode

Monitoring mode

Usage Guidelines

Max: means the maximum power limitation of a port

Current: means the current power of a port

Average: means the average power of a port, which is effective only when the power statistics table is enabled

Peak: means the peak power of a port, which is effective when the power statistics is enabled

Bottom: means the bottom power of a port, which is effective only when the power statistics table is enabled

Example

Switch#show poe power

Port	Current	Max	Average	Peak	Bottom
f0/3	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/4	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/2	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/1	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/5	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/6	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/7	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/8	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/9	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/10	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/11	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/12	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/13	7600 mW	30000 mW	7620 mW	7800 mW	7600 mW
f0/14	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/15	7600 mW	30000 mW	7600 mW	7800 mW	7600 mW

f0/16	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/17	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/18	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/19	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/20	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/21	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/22	15900 mW	30000 mW	15890 mW	16200 mW	14900 mW
f0/23	7700 mW	30000 mW	7780 mW	7800 mW	7700 mW
f0/24	8400 mW	30000 mW	9850 mW	22500 mW	6500 mW

Related Command

None

52.1.4 show poe interface

Syntax

It is used to display the detailed POE information of a designated port

show poe interface *type slot/port*

Parameter

Parameter	Description
type	Interface type
slot	Slot ID
port	Port ID

Default

None

Command Mode

Monitoring mode

Usage Guidelines

PSE Port Number: means the ID of an internal port

Port Power Enabled: means to enable the power supply for a port

Port Force Power: means to enable the forced power supply or the power supply for a low-priority port

Port Detection Status: the power supply state of a port, which may be disabled, searching, delivering-power or fault

Port Fault Status: means the error information about a port

Port Last Disconnection Reason: means the reason of the latest power cutoff on a port

Port pairs: means the ordering of the power line of a port, of which **signal** means the power supply by way of the signal line and **spare** that by way of the spare line

Port IEEE Class: means the class of a port

Port priority: means the priority for port's power supply and it from high to low is critical, high and low

Port Current: stands for the present current on a interface

Port Voltage: means the current voltage of a port, which cannot be shown by some chips

Port Current Power: stands for the current power on an interface

Port Average Power: means the average power of a port, which is effective only when the power statistics table is enabled

Port Peak Power: means the peak power of a port, which is effective when the power statistics is enabled

Port Bottom Power: means the bottom power of a port, which is effective only when the power statistics table is enabled

Port Max Power: means the maximum power limitation of a port

Port PD Description: stands for the description of a port

Example

Switch#show poe interface f0/24

PSE Port Number : 23

Port Power Enabled : enable

Port Force Power : disable

Port Detection Status : delivering-power

Port Fault Status :

Port Last Disconnection Reason : Port was disabled

Port Pairs : signal

Port IEEE Class : 0

Port Priority : critical

Port Current : 163 mA

Port Current Power : 8400 mW

Port Average Power : 8440 mW

Port Peak Power : 22500 mW

Port Bottom Power : 6500 mW

Port Max Power : 30000 mW

Port PD Discription : AP

Related Command

None

52.1.5 poe disable

Syntax

Enabling the Power Supply of a Port

poe disable { time-range *name* /<cr>}

no poe disable {time-range /<cr>}

Parameter

Parameter	Description
time-range *name*	The parameter name stands for the **name** of the power-off time range
<cr>	Means to enter **poe disable** alone and shut down the port

Default

Power supply on a port is enabled and there is no time limit to power supply

Command Mode

Interface configuration mode

Usage Guidelines

poe disable: means to shut down power supply

no poe disable: means to open power supply

poe disable time-range name: means to add the period control of disabling power supply in the period of name

no poe disable time-range: means to cancel the period control of disabling power supply in the period

Example

The following example shows how to disable the power supply of port f0/1

Switch_config_f0/1#poe disable

The following example shows how to disable the power supply in the period named Sunday_free

Switch_config_f0/1poe disable time-range Sunday_free

Related Command

time-range

52.1.6 poe max-power

It is used to set the maximum power of a port

poe max-power *value*

no poe max-power

Parameter

Parameter	Description
value	Means the maximum power of a port, whose unit is mW

Default value

The default maximum power of a port is 30000mW

Command mode

Interface configuration mode

Explanation

The "no" form of this command can be used to resume the default maximum power

Example

The following example shows how to set the maximum power of port f0/1 to 15000mW

Switch_config_f0/1#poe max-power 15000

52.1.7 poe priority

Setting the Power Supply Priority for a Port

poe priority {critical | high | low }

Parameter

Parameter	Description
critical	Stands for the highest priority
high	Stands for the high priority
low	Stands for the lowest priority

Default value

The power supply priority of a port is **low** by default

Command mode

Interface configuration mode

Explanation

The "no" form of this command can be used to resume the default port priority

Example

The following example shows how to set the power supply priority of port f0/1 to **critical**

Switch_config_f0/1#poe priority critical

Remark

Some PoE chips do not support this command

52.1.8 poe PD-discription

Syntax

It is used to set the port description (usually for PD)

poe PD-discription *string*

no poe PD-discription

Parameter

Parameter	Description
string	Stands for the character string of port's description

Default

The default value is null

Command Mode

Interface configuration mode

Usage Guidelines

The "no" form of this command is used to delete the description character string

Example

The following example shows how to set POE description of port f0/1 to AP-1

Switch_config_f0/1#poe PD-discription **AP-1**

Related Command

None

52.1.9 poe force-power

Syntax

It is used to set the forced power supply

poe force-power

no poe force-power

Parameter

None

Default

The forced power supply is disabled by default

Command Mode

Interface configuration mode

Usage Guidelines

The "no" form of this command is used to disable the forced power supply

Example

The following example shows how to set the forced power supply for the POE port of interface f0/1

Switch_config_f0/1#poe force-power

Related Command

poe power-management

Remark

Some PoE chips do not support this command

52.1.10 poe inrush

Syntax

To configure the port poe inrush high, run the following command:

poe inrush high

no poe inrush

Parameter

None

Default

disabled

Command Mode

Interface configuration mode

Usage Guidelines

The "no" form of this command is used to disable the port poe inrush high

Example

The following example shows how to configure the POE port of port f0/1 to support high inrush:

Switch_config_f0/1#poe inrush high

Remark

Some PoE chips do not support this command

52.1.11 poe extern-power

Syntax

To configure poe extra power, run the following command:

poe extern-power *value [slot]*

no poe extern-power *[slot]*

Parameter

Parameter	Description
value	Power, in W
slot	Slot number, no need for stand-alone

Default

None

Command Mode

Global configuration mode

Usage Guidelines

Stand-alone machine: poe extern-power 300 means that the poe power of the whole machine is additionally increased by 300W

Stacking: poe extern-power 300 1/0 means that the poe power of member 1/0 increases by an additional 300W

After the configuration, use **show poe system** to see if the power increases

Example

The following example shows how to increase the poe power of the whole machine by 300W:

Switch_config#poe extern-power 300

Related Command

show poe system

52.1.12 poe perpetual

Syntax

To configure poe hot restart without power failure, run the following command:

poe perpetual *[slot]*

no poe perpetual *[slot]*

Parameter

Parameter	Description
slot	Slot number, no need for stand-alone

Default

disable

Command Mode

Global configuration mode

Usage Guidelines

Stand-alone machine: poe perpetual means that the poe port is always powered on during a warm restart

Stacking: poe perpetual 1/0 indicates that the poe port is always powered on when member 1/0 is hot restarted

Some poe chips do not support this function

Example

The following example shows how to configure a hot restart without power loss:

Switch_config#poe perpetual

52.1.13 poe detection

Syntax

To configure poe detection mode, run the following command:

poe detection <RES|RES-CAP> *[slot]*

Parameter

Parameter	Description
RES	Resistance detection
RES-CAP	Capacitance detection
slot	Slot number, no need for stand-alone

Default

The default is resistance detection

Command Mode

Global configuration mode

Usage Guidelines

Stand-alone machine: poe detection RES-CAP means that the POE chip uses the capacitance detection method to check whether the power is supplied

Stacking: poe detection RES-CAP 1/0 indicates that the POE chip of member 1/0 uses the capacitance detection method to check whether it is powered

Some poe chips do not support this function

Example

The following example shows how to configure the capacitance detection mode:

Switch_config#poe detection RES-CAP

Chapter 53 Private VLAN Configuration Commands

53.1 private-vlan

Syntax

private-vlan {primary|community|isolated}

To configure the features of private VLAN, run the aforementioned command

Parameter

Parameter	Description
primary	Sets VLAN to the primary VLAN
community	Sets VLAN to the community VLAN
isolated	Sets VLAN to the isolated VLAN

Default value

No configuration is done to any type of private VLAN

Command mode

VLAN configuration mode

Usage guidelines

Primary VLAN: It is relevant to a promiscuous port and only one primary VLAN exists in the private VLAN. Each port in the primary VLAN is a member in the primary VLAN

Isolated VLAN: No layer-2 communication can be conducted between two ports in the same isolated VLAN. Also, there is only one isolated VLAN in a private VLAN. The isolated VLAN must be related with the primary VLAN

Community VLAN: Layer-2 communication can be conducted between two ports in the same VLAN, but they have no communication with the ports in another community VLAN. One private VLAN may contain multiple community VLANs. The community VLAN must be related with the primary VLAN

Example

The following example shows how to set VLAN2 to be the primary VLAN

Switch_config#

Switch_config#vlan 2

Switch_config_vlan2#private-vlan primary

53.2 private-vlan association

Syntax

private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}

no private-vlan association

To configure the private VLAN's association, run the first one of the above-mentioned commands

Parameter

Parameter	Description
svlist	Sets the to-be-associated secondary VLAN

Default value

No secondary VLAN is associated

Command mode

VLAN configuration mode

Usage guidelines

This command is used to associate primary VLAN with secondary VLAN to enable them to realize VLAN learning sharing in the whole private VLAN. This command is run only in primary VLAN configuration mode

When svlist is used, you can add or remove the lists to or from secondary VLAN. The entered lists are separated by the comma or the hyphen. For example, "1, 3, 5, 7" stands for "vlan 1, vlan 3, vlan 5, vlan 7", while "1, 3-5, 7" stands for "vlan 1, vlan 3, vlan 4, vlan 5, vlan 7"

The validation of the whole private VLAN depends on the correct configurations of all features in private VLNA

Example

The following example shows how to associate primary VLAN 2 with community VLAN 3 or community VLAN 4

Switch_config#

Switch_config#vlan 2

Switch_config_vlan2#private-vlan association 3-4

53.3 switchport mode private-vlan

Syntax

switchport mode private-vlan {*host* | *promiscuous*}

To set the mode for a layer-2 port in private VLAN, run the above-mentioned command

Parameter

Parameter	Description
host	Sets the layer-2 port to be in host's port mode
promiscuous	Sets the layer-2 port to be in promiscuous port mode

Default value

No mode in any private VLAN is configured

Command mode

Port configuration mode

Usage guidelines

This command is used to set the mode in private VLAN for layer-2 port: the promiscuous port mode or the host port mode. The latter can be classified into the public port and the isolated port

Promiscuous port: it belongs to the primary VLAN. It can communicate with all other ports, including the isolated port and community port of a secondary VLAN in the same private VLAN

Isolated port: It is the host port in the isolated VLAN. In the same private VLAN, the isolated port is totally L2 isolated from other ports except the promiscuous port, so the flows received from the isolated port can only be forwarded to the promiscuous port

Community port: It is the host port in the community VLAN. In a private VLAN, the community ports of the same community VLAN can conduct L2 communication each other or with the promiscuous port, but not with the community ports of other VLANs and the isolated ports in the isolated VLANs

Example

The following example shows how to set interface g0/1 to a promiscuous port:

Switch_config#

Switch_config#interface g0/1

Switch_config_g0/1#switchport mode private-vlan promiscuous

53.4 switchport private-vlan host-association

Syntax

switchport private-vlan host-association *p_vid s_vid*

To set the private VLAN associating with the L2 host port, run the above-mentioned command

Parameter

Parameter	Description

p_vid	Sets the VLAN ID of the to-be-associated primary VLAN, which ranges between 1 and 4094
s_vid	Sets the VLAN ID of the to-be-associated secondary VLAN, which ranges between 1 and 4094

Default value

No association is set for private VLAN

Command mode

Port configuration mode

Usage guidelines

This command is mainly used to set the L2 host port to associate primary and secondary VLANs. This newly configured host port takes no effect on the associated primary and secondary VLANs until you set it to be the host port, the private VLAN type of the two associated VLANs is set correctly and the association of the two VLANs is correctly set

Example

The following example shows how to build up the host association between port g0/1 and primary VLAN2 and secondary VLAN3

Switch#config

Switch_config#interface g0/1

Switch_config_g0/1#switchport private-vlan host-association 2 3

53.5 switchport private-vlan mapping

Syntax

switchport private-vlan mapping

p_vid{*svlist* | **add** *svlist* | **remove** *svlist*}

To set the private VLAN associating with the L2 promiscuous port, run the above-mentioned command

Parameter

Parameter	Description
p_vid	Sets the VLAN ID of the to-be-associated primary VLAN, which ranges between 1 and 4094.
svlist	Sets the to-be-associated secondary VLAN.

Default value

No association is set for private VLAN

Command mode

Port configuration mode

Usage guidelines

This command is mainly used to set the L2 promiscuous port to associate primary and secondary VLANs. This newly configured port takes no effect on the associated primary and secondary VLANs until you set it to be the promiscuous port, the private VLAN type of the two associated VLANs is set correctly and the association of the two VLANs is correctly set

When svlist is used, you can add or remove the lists to or from secondary VLAN. The entered lists are separated by the comma or the hyphen. For example, “1, 3, 5, 7” stands for "vlan 1, vlan 3, vlan 5, vlan 7”, while “1, 3-5, 7” stands for "vlan 1, vlan 3, vlan 4, vlan 5, vlan 7”

Example

The following example shows how to build up the promiscuous association between port g0/1 and primary VLAN2 and secondary VLANs 3-5

Switch#config

Switch_config#interface g0/1

Switch_config_g0/1#switchport private-vlan mapping 2 3-5

53.6 switchport private-vlan

Syntax

switchport private-vlan { tag-pvid *p_vid* **| tag-pri** *priority* **| untagged }**

no switchport private-vlan untagged

To set the tag and its field of the egress packets on the L2 port of the private VLAN, run the first of the above-mentioned two commands

Parameter

Parameter	Description
p_vid	Stands for the VLAN ID in the tag, which ranges from 1 to 4094
priority	Sets the priority field in the tag, which ranges from 0 to 7
untagged	Sets the egress packets to have the tag or not.

Default value

The default VLAN ID in the tag is 1

The default priority is 0

The egress has no tag by default

Command mode

Port configuration mode

Usage guidelines

This command is mainly used to set the tag of egress packets in private VLAN or set whether egress packets have the tag. This command takes effect after private VLAN, the association between private VLANs in the private VLAN domain, the L2 port mode in private VLAN, and the association between L2 port and private VLAN are all correctly set

53.7 show vlan private-vlan

Syntax

show vlan private-vlan

To display the configurations of VLAN and L2 port in the private VLAN, run the above-mentioned command

Parameter

N/A

Default value

N/A

Command mode

Port configuration mode, VLAN configuration mode and EXEC mode

Usage guidelines

This command is used to display the configurations of VLAN and L2 port in the private VLAN

Example

The following example shows how to display the configuration of private VLAN

```
Switch_config#

Switch_config#show vlan private-vlan

Primary  Secondary  Type              Ports

-------  ---------  ----------------  ------------------------------------------

2        3          community         G0/1, G0/2, G0/3

2        4          isolated          G0/1, G0/4

2        5          community         G0/1, G0/5
```

53.8 show vlan private-vlan interface

Syntax

show vlan private-vlan interface *interface*

To display the configurations of the L2 port in the private VLAN, run the above-mentioned command

Parameter

Parameter	Description
Interface	Stands for the to-be-shown interface

Default value

N/A

Command mode

Port configuration mode, VLAN configuration mode and EXEC mode

Usage guidelines

This command is used to display the configuration of L2 port in the private VLAN

Example

The following example shows how to display the configuration of L2 interface g0/1 in the private VLAN

Switch_config#

Switch_config#show vlan private-vlan interface g0/1

port type: promiscuous port

private-vlan host-association: primary vlan 2 secondary vlan 3

private-vlan mapping: primary vlan 2 secondary vlan 3-5

Native VLAN tagging enable: untagged

Native VLAN tagging priority 0

Native VLAN tagging pvid: 1

Chapter 54 QoS Configuration Commands

54.1 cos default

Syntax

To configure the default value of CoS, use the **cos default** command. To disable the configuration, use the no form of this command

cos default *cos*

no cos default

Parameter

Parameter	Description
cos	Default cos value. The range is 0-7

Default

The default CoS value is 0

Usage Guidelines

Use the command in layer-2 port configuration mode and global configuration mode

In global configuration mode, the command will configure the default CoS value of all ports. However, in layer-2 port configuration mode, the command will only configure the default CoS value of the configured port

Example

The following example shows how to set the cos value received in interface g0/1 to 4:

Switch_config#inter g0/1

Switch_config_g0/1#cos default 4

54.2 cos map

Syntax

cos map *quid cos1..cosn*

no cos map

To set the CoS priority queue according to the priority, use the **cos map** command. To disable the configuration, use the no form of this command

Parameter

Parameter	Description
quid	Stand for CoS priority queue ID, the range is from 1 to 8
cos1..cosn	Stand for CoS value defined by IEEE802.1p, the range is from 0 to 7

Default

CoS value	S priority queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Usage Guidelines

Layer 2 port configuration mode and global configuration mode

Using this command in the global configuration mode, the CoS priority queue of all ports will be affected. Using this command under the Layer 2 port will only affect the CoS priority queue of the port

Example

The following example shows how to map CoS 0-2 to CoS priority queue 1, and CoS 3 to priority queue 2

Switch_config # cos map 1 0 1 2

Switch_config # cos map 2 3

54.3 dscp map

Syntax

dscp map *word* {**cos** *cos-value*}

no dscp map

To set the CoS priority queue according to dscp, use the **dscp map** command. To disable the configuration, use

the no form of this command

Parameter

Parameter	Description
word	Stand for Dscp range table, such as (1, 3, 5, 7), (1, 3-5, 7), (1-7).
cos *cos-value*	Stand for Dscp mapping priority cos, the range is from 0 to 7.

Default

None

Usage Guidelines

Configure the command in global configuration mode

Example

The following example shows how to map dscp 0-2 to CoS priority queue 1

Switch_config#dscp map 0-2 cos 1

54.4 scheduler weight bandwidth

Syntax

To set the weight of the wrr queues, use the first one of the following commands. To return to the default value, use the no form of this command

scheduler weight bandwidth *weight1...weightn*

no scheduler weight bandwidth

Parameter

Parameter	Description
weight1...weight8	Stand for the weights of 8 CoS priority queues of WRR/DRR. 0-127

Default

The weight of each queue is 1

Usage Guidelines

Use the command in layer-2 port configuration mode and global configuration mode

If this command is run in global configuration mode, the bandwidth of all priority queues on all interfaces are affected. If this command is run in layer-2 port configuration mode, only the bandwidth of the priority queues on its interfaces are affected. This command validates only when the queue schedule mode is set to WRR. This command decides the bandwidth weight value of the CoS priority queue when the WRR schedule policy is used

The weight of the third queue and following queues can be assigned to 0. Once the weight of a queue is assigned to 0, the following queue weight will be forced to 0. In this case, mixing mode is used

Example

The following example shows how to set the weight values of eight CoS priority queues to 1, 2, 3, 4, 5, 6, 7 and 8 respectively

Switch_config # scheduler weight bandwidth 1 2 3 4 5 6 7 8

54.5 scheduler policy

Syntax

scheduler policy { **sp** | **wrr | wfq | fcfs** }

no scheduler policy

To set CoS priority queue scheduler policy, use the scheduler policy command

Parameter

Parameter	Description
sp	Use the sp debug stratefgy
wrr	Use the wrr debug strategy
wfq	Use the wfq debug strategy
fcfs	Use the fcfs debug strategy

Default

Use SP

Usage Guidelines

Use the command in layer-2 port configuration mode and global configuration mode

If this command is run in global configuration mode, the queue debug policy of all ports are affected. If this command is run in port configuration mode, only the queue debug policy of its port are affected. There is no **fcfs** command in port configuration mode

After configure the command, the interface send debug mode is configured to specified value.

Example

The following example shows how to set configure interface send debug mode as wrr:

Switch_config # scheduler policy wrr

54.6 policy-map

Syntax

To set QOS policy-map, use the policy-map command

policy-map *name*

no policy-map *name*

Parameter

Parameter	Description
name	Name of the policy map , the value range is 1 to 20 characters

Default

None

Usage Guidelines

Global configuration mode

After inputting this command, the system will enter QoS policy mapping configuration mode. There are following commands in this mode:

- **classify**: It is used to configure QoS flow
- **description**: It is used to describe QoS policy mapping
- **exit**: It is used to quit from QoS policy mapping configuration mode
- **no**: It is used to cancel the command that formerly inputs
- **action**: It is used to define QoS action

Example

The following example shows how to configure QoS policy map:

Switch_config # policy-map myqos

54.7 classify

Syntax

To configure the matching data traffic of QoS policy, use the classify command

classify {**any** | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp** *dscp-value* | **tos** *tos-value* | **diffserv** *diffserv-value* | **ip** *ip-access-list* | **ipv6** *ipv6-access-list* | **mac** *mac-access-list* }

no classify { **cos** | **icos** | **vlan** | **ivlan** | **ethernet-type** | **precedence** | **dscp** | **tos** | **diffserv** | **ip** | **ipv6** | **mac** }

Parameter

Parameter	Description
any	match any data packets
cos *cos*	Configures the matching COS value; the valid range is 0 to 7
icos *icos*	Configures the matching interior tag COS value; the valid range is 0 to 7
vlan *vlanid*	Configures the matching VLAN; the valid range is 1 to 4094
ivlan *ivlanid*	Configures interior tag vlan id. 1-4094
ethernet-type *ethernet-type*	Configures the matching Ethernet type, 0x0600-0xFFFF
precedence *precedence-value*	The priority field in tos of ip packet (5-7 of tos), 0-7
dscp *dscp-value*	Dscp field in tos of ip packet (2-7 of tos), 0~63
tos *tos-value*	tos in the ip packet represents delay, throughput, reliability and cost field (1-4 of tos), 0~15
diffserv *diffserv-value*	All tos field in Ip packet: 8, 0-255
ip *ip-access-list*	Configures the matching IP access list name; the range is 1 to 20 characters
ipv6 *ipv6-access-list*	Configures the matching IPV6 access list name. The valid range is 1 to 20 characters
mac *mac-access-list*	Configures the matching MAC access list name. The valid range is 1 to 20 characters

Default

Match any data packets

Usage Guidelines

QoS policy map configuration mode

All data flows in a QoS policy table must have the same mask value, and the port number in the ip access-list must be determined, not a range

The permit rules in the IP access list and MAC access list used to match the data flow are valid, that is, the permit rule is used to match the data flow, and the deny rule is not used to configure the data flow

When the **qinq** mode is enabled, that is, after the **dot1q-tunnel** command is configured, the downlink interface matches the vlan or cos value of the source packet with ivlan and icos values

Example

Switch-policy-map#classify vlan 4

54.8 action

Syntax

To configure the matching data traffic policy of QoS policy map, use the action command

action{**bandwidth** *max-band* | **cos** *cos* | **drop** | **dscp** *dscp-value* | **precedence** *precedence-value* | **forward** | **icos** *icos* | **ivlanID** { **add** *addivlanid* | *ivlanid*}| **monitor** *session-value* | **quequ** *quequ-value* | **redirect** *interface-id* | **stat-packet** | **stat-byte** | **vlanID** { **add** *addvlanid* | *vlanid*} | **copy-to-cpu**}

no action {**bandwidth** | **cos** | **drop** | **dscp** | **precedence** | **forward** | | **icos** | **ivlanID** | **monitor** | **quequ** | **redirect** | **stat-packet** | **stat-byte** | **vlanID** | **copy-to-cpu**}

Parameter

Parameter	Description
bandwidth *max-band*	Maximum bandwidth to a class, the range is 1 to 163840. Unit: 64Kbps
cos *cos*	Sets cos field as cos-value 0~7
drop	Drops the configured packets
dscp *dscp-value*	Define the dscp field of the matching traffic as dscp-value; the range is 0 to 63
precedence *precedence-value*	Sets tos priority field of the matching flow ip packets (5~7 of tos). The range is 0-7
forward	No operation for the matching packet
icos *icos*	Configures the matching interior tag COS value; the valid range is 0 to 7
ivlan {**add** *ivlanid*	*ivlanid*}	Configures to replace or add interior tag vlan id. 1-4094
monitor *session-value*	Send the packets to monitor interface; the range is 1-4
queue *queue-value*	Sets mapping queue; the range is 1-8
redirect *interface-id*	Redirects the exit of the matching traffic
stat-packet	Calculate the number of packets
stat-byte	Calculate the number of bytes
vlanID { **add** *vlanid* / *vlanid* }	Sets replacing or adding exterior vlanid; the range is 1-4094
copy-to-cpu	Forward to CPU simultaneously

Default

None

Usage Guidelines

QoS policy map configuration mode

vlan and cos can be effective on the non-dot1q-tunnel-uplink interface when ivlan and icos are configured

A policymap needs to be configured independently when Monitor is applied on the egress, or the result is abnormal

In ingress direction, vlan, ivlan cannot configure with dscp, precedence, bandwidth, cir, mirror, stat, redirect

In ingress direction, cos, icos cannot configure with dscp, precedence, bandwidth, cir, mirror, stat, redirect

In egress direction, cos, icos cannot configure with dscp, precedence, bandwidth, cir, mirror, stat, redirect

Example

Switch-policy-map#action redirect g0/1

54.9 qos policy

Syntax

To configure the QoS policy on interface, use the qos policy command

[**no**] **qos policy** *name* { **ingress**}

Paramter

Parameter	Description
name	Name of QoS policy maps
ingress	Affect the entrance

Deault

None

Usage Guidelines

Use the command in layer-2 port configuration mode and global configuration mode

When applied in egress direction, for most actions, the incoming flow must be a known unicast to correctly match

Example

Apply the QoS policy named pmap on the interface g0/1:

Switch_config#inter g0/1

Switch_config_g0/1# qos policy pmap ingress

54.10 show policy-map

Syntax

show policy-map {*policy-map-name* / **interface** [*interface-id*] | **global** }

Displays all or some designated QoS policy maps

Parameter

Parameter	Description
policy-map-name	Stands for the name of a QoS policy map
interface [*interface-id*]	Displays the QoS strategy of a port
global	Global configuration strategy

Default

None

Usage Guidelines

None

Example

The following example displays all QoS strategy mapping tables

```
Switch_config#show policy-map
policy-map          1
    classify any
    action redirect g0/1
policy-map          11
    classify any
    action
Switch_config#
```

54.11 trust

Syntax

[**no**]**qos trust** { *cos* | *dscp* | *untrust* }

To configure in trust mode, use **qos trust** command

Parameter

Parameter	Description
cos	Modes of trust
dscp	Trust mode
untrust	Untrust mode

Default

None

Usage Guidelines

Use the command in global configuration mode

Example

The following example shows how to configure trust cos:

Switch_config#qos trust cos

Chapter 55 VRRP Configuration Commands

55.1 vrrp associate

Syntax

To configure the virtual IP address of VRRP, run the following command

vrrp [*vrid***] associate** *virtual-address virtual-mask* **[secondary]**

To return to the default setting, use the no form of this command

no vrrp [*vrid***] associate [***virtual-address virtual-mask***] [secondary]**

Parameter

Parameter	Description
vrid	The virtual routing switch ID. The value ranges from 0 to 255. The default value is 0
virtual-address	The virtual IP address
virtual-mask	The virtual IP address mask

Default Value

Disabled

Usage Guidelines

The virtual IP address must be in the same network range of the interface IP, or the virtual routing switch won't work

When the virtual IP address is identical to the interface IP address, the system will automatically advance routing switch to 255

The virtual routing switch may configure multiple IP addresses, among which one is as the master address and the others are as secondary address. The virtual IP secondary address is configured by command with secondary parameters

Example

The following example shows how to enable vrrp group 1 on interface vlan 1 and the configured virtual IP address is 192.168.20.100:

Switch_config_v1#vrrp 1 associate 192.168.20.100 255.255.255.0

55.2 vrrp authentication

Syntax

To configure simple-text authentication method of interface VRRP, run the following command

vrrp [*vrid***] authentication** *WORD*

To return to the default setting, use the no form of this command

no vrrp [*vrid***] authentication**

Parameter

Parameter	Description
vrid	ID of the virtual routing switch. The value ranges from 0 to 255. The default value is 0
WORD	The verification plaintext. The length cannot exceed 8 characters

Default Value

no authentication

Usage Guidelines

The virtual routing switch group which makes up of the virtual routing switch must have the identical authentication method

Example

The following example configures authentication method of the virtual routing switch 1 on interface vlan 1 to simple-text and the authentication character string is test:

Switch_config_v1#vrrp 1 authentication test

55.3 vrrp description

Syntax

To configure the description information of VRRP, run the following command:

vrrp [*vrid***] description** *WORD*

To return to the default setting, use the no form of this command

no vrrp [*vrid***] description**

Parameter

Parameter	Description
vrid	The virtual routing switch ID. The value ranges from 0 to 255. The default value is 0
WORD	The description character string. The length cannot outnumber 64 characters

Default Value

No description

Usage Guidelines

None

Example

The following example shows how to configure the description information of the virtual routing switch 1 on switch VLAN1 interface to GROUP1:

Switch_config_v1# vrrp 1 description GROUP1

55.4 vrrp preempt

Syntax

To configure Virtual Router Redundancy Protocol (VRRP) preempt, run the following command. To return to the default setting, use the no form of this command

vrrp [*vrid*] preempt

no vrrp [*vrid*] preempt

Parameter

parameter	Description
vrid	ID of the virtual routing switch. The value ranges from 0 to 255. The default value is 0

Default Value

Enabled

Command Mode

VLAN interface configuration mode

Usage Guidelines

When VRRP preempt is enabled, the high priority switch in the virtual routing switch of the same group will preempt that of the low priority. When VRRP preempt is disabled, the high priority switch will not preempt that of the low priority

Example

The following example disables preempt of virtual routing switch 1 on interface vlan 1:

Switch_config_v1# no vrrp 1 preempt

55.5 vrrp preempt delay

Syntax

To configure the priority preempt delay of VRRP, run the following command

vrrp [*vrid*] **preempt delay** *second*

To return to the default setting, use the no form of this command

no vrrp [*vrid*] **preempt delay** *second*

Parameter

Parameter	Description
vrid	The virtual routing switch ID, The value ranges from 0 to 255. The default value is 0
second	The priority preempt delay, 0 to 255, unit: second

Default Value

The priority preempt delay is 0 second

Usage Guidelines

None

Example

The following example shows how to set the priority preempt delay of the virtual routing switch 1 on the switch VLAN interface to 10 seconds

Switch_config_v1# vrrp 1 preempt delay 10

55.6 vrrp priority

Syntax

To configure Virtual Router Redundancy Protocol (VRRP) priority value, run the following command. To return to the default setting, use the no form of this command

vrrp [*vrid*] **priority** *value*

no vrrp [*vrid*] **priority**

Parameter

Parameter	Description
vrid	ID of virtual routing switch. The value ranges from 0 to 255. The default value is 0

value	Priority value. The value ranges from 1 to 254

Default Value

100

Usage Guidelines

None

Example

The following example configures priority value of the virtual routing switch 1 on interface vlan 1 to 120.

Switch_config_v1#vrrp 1 priority 120

55.7 vrrp source-mac-use-system

Syntax

To configure the source mac address of the VRRP protocol packet, run the following command. To return to the default setting, use the no form of this command

[no] vrrp [*vrid*] source-mac-use-system

Parameter

Parameter	Description
vrid	The virtual routing switch ID. The value ranges from 0 to 255. The default value is 0

Default Value

The protocol mac address is used by default

Usage Guidelines

After the command is configured, VRRP packet will use the system mac as the source mac address of the protocol packet

Example

The following example shows how the virtual routing switch1 of VLAN1 interface forwards the protocol packet by the system mac address

Switch_config_v1#vrrp 1 source-mac-use-system

55.8 vrrp timers

Syntax

vrrp [*vrid*] **timers advertise** {*second* | **dsec** *decisecond* | **csec** *centisecond*}

no vrrp [*vrid*] **timers advertise**

To configure announce timer of vrrp, run the following command. To return to the default setting, use the no form of this command

vrrp [*vrid*] **timers learn**

no vrrp [*vrid*] **timers learn**

To configure announce timer to the learning mode, run the following command. To return to the default setting, use the no form of this command

Parameter

Parameter	Description
vrid	ID of virtual routing switch. The value ranges from 0 to 255. The default value is 0
second	Announce timer value; unit: second; the value ranges from 1 to 255
decisecond	Announce timer value, unit: 0.1s; the value ranges from 5 to 360
centisecond	Announce timer value, unit: 0.01s; the value ranges from 1 to 3600

Default Value

1 sec

Usage Guidelines

The timer value will decide the minimum time that the virtual routing switch recovers from the error. When the link of the master routing switch is down, the backup routing switch will transit to master routing switch in 3*advertisement + skew_time interval. The large value of the advertisement is obviously nor favorable for error recovery. We recommend user to use the default value

When configured in learning mode, the virtual routing switch will learn the announce clock value from the message of the master routing switch

Example

The following command configures announce timer value of virtual routing switch 1 on interface vlan 1 to 2 seconds:

Switch_config_v1#vrrp 1 timers advertise 2

55.9 vrrp track

Syntax

To configure VRRP monitoring function, run the following command. To return to the default setting, use the no form of this command

vrrp [*vrid*] **track interface** *intf-id value*

no vrrp [*vrid*] **track interface** *intf-id*

vrrp [*vrid*] **track ip** *ip-address value*

no vrrp [*vrid*] **track ip** *ip-address*

To configure BFD static detection, run the following command. If next jump is reachable, the objective node route is reachable. To return to the default setting, use the no form of this command

ip route bfd static next-hop

no ip route bfd static next-hop

To configure BFD detection static routing function, run the following command. If the configured gateway address is reachable, the objective node route is reachable. To return to the default setting, use the no form of this command

ip route bfd static *A.B.C.D*

no ip route bfd static *A.B.C.D*

Parameter

Parameter	Description
vrid	The virtual routing switch ID. The value ranges from 1 to 255. The default value is 0
intf-id	The concrete physical port of the monitor
ip-address	The IP address of the monitor node
value	The priority penalty value. The value ranges from 1 to 254. The configured penalty value should not be greater than the priority of the current vrrp group
A.B.C.D	The gateway address when BFD detecting the static routing

Default Value

None

Usage Guidelines

With the monitoring function, VRRP group can appropriately adjust its priority according to the link state change and provide an opportunity of switching the main line state to the backup line state. The link state change refers to the destination link passing through VRRP routing switch is reachable or not, rather than that of VRRP routing switch itself

VRRP supports two monitoring objects. First, monitoring interface state. When the monitored interface link state is down, lower the priority itself actively; second, monitor the static routing state of the designated node. When the monitored route is unreachable, lower the priority itself actively. Monitoring the static routing state of the designated node needs BFD static route detection function

Example

The following example shows how to set vlan1 virtual routing switch1 monitoring the physical port g5/1. When the physical port g5/1 state is down, lower itself priority 20

Switch_config_v1#vrrp 1 track interface GigaEthernet0/1 20

The following example shows how vlan1 port virtual routing switch 1 monitors the static routing state of IP address 1.1.1.254. After the corresponding static route and BFD is configured and the routing state of 1.1.1.254 is unreachable, lower itself priority 20:

Switch_config#ip route 1.1.1.254 255.255.255.255 1.1.1.100

Switch_config#ip route bfd static next-hop

Switch_config_v1#vrrp 1 track ip 1.1.1.254 20

55.10 show vrrp

Syntax

To display Virtual Router Redundancy Protocol (VRRP) information, run the following command. To return to the default setting, use the no form of this command

show vrrp brief

show vrrp [**interface** *intf-id*] **detail**

Parameter

Parameter	Description
intf-id	The concrete physical interface

Default Value

None

Usage Guidelines

The command is used to show VRRP information

Example

The following example displays vrrp information on interface vlan 1:

Switch_config#show vrrp interface vlan 1 detail

VLAN1 - Group 1

VRRP State is Master

Virtual IP address : 192.168.20.110/24

Virtual Mac address : 0000.5e00.0101

Current Priority : 100 (Config 100)

VRRP timer : Advertise 1.0 s (default) master_down 3.6 s

VRRP current timer : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s

Authentication string is not set

Preempt is set (delay : 0 s)

Learn Advertise Interval is not set

Master Router IP : 192.168.20.118, priority : 100, advertisment : 1.0 s

55.11 debug vrrp

Syntax

To enable debugging VRRP information, use the debug vrrp command. Use the no form of this command to disable debugging VRRP information

debug vrrp [interface *intf-id vrid***] {errors | events | packets | all}**

no debug vrrp

Parameter

Parameter	Description
intf-id	Concrete physical port
vrid	Virtual routing switch ID. The value ranges from 0 to 255. The default value is 0

Default Value

Disabled

Usage Guidelines

None

Example

The following command shows how to enable VRRP debugging switch:

Switch# debug vrrp packets

Chapter 56 RNP Configuration Commands

56.1 bvss rnp old-master-timeout

Syntax

To configure the timeout of the RNP old master device, run the following command. To restore the default value, run the no form of the command

bvss rnp old-master-timeout *value*

no bvss rnp old-master-timeout

Parameters

Parameter	Description
value	The timeout value of the RNP old master device, range: 3-10 minutes

Default Value

3 minutes

Usage Guidelines

None

Example

The following command shows how to configure the timeout value of the RNP old master device to 10 minutes:

Switch_config#bvss

Switch_config_bvss#bvss rnp old-master-timeout 10

56.2 show bvss rnp

Syntax

To show RNP state information, run the following command

show bvss rnp

Parameters

None

Default Value

None

Usage Guidelines

None

Example

None

Chapter 57 VRF Configuration Commands

57.1 ip vrf vrf-name

Syntax

To configure VRF, enter the VRF configuration mode. To return to the default setting, use the no form of this command

ip vrf *vrf-name*

no ip vrf *vrf-name*

Parameter

vrf-name	Name of VRF

Default value

None

Command mode

Routing configuration mode

Usage guidelines

If VRF is created, use command **ip vrf vrf-name** to enter VRF configuration mode and VRF will not be created again, vice verse

Use command no **ip vrf vrf-name** to delete all configurations of VRF. Delete VRF table and VRF configuration of relevant ports but sitemap configuration will not be deleted

Example

The following example shows how to create VRF named PE

R1_config#ip vrf PE

Related command

rd

57.2 description

Syntax

To configure VRF description, run the following command.

description *LINE*

no **description**

Parameter

LINE	Description shall be 79 characters at most

Default value

None

Command mode

VRF configuration mode

Usage guidelines

Example

The following example shows how to configure description of VRF named PE

R1_config#ip vrf PE

R1_config_vrf_PE#description this is description for pe vrf

Related command

ip vrf vrf-name

57.3 export map

Syntax

To configure expand attribute the route carries with which VRF sends out, run the following command. To return to the default setting, use the no form of this command

export map *WORD*

no **export map** *WORD*

Parameter

WORD	name of route-map

Default value

None

Command mode

VRF configuration mode

Usage guidelines

When using the command **export map** ***WORD***, if the corresponding VRF is not configured with export map, the export map name of VRF is that of route-map. If export map is configured with a different name, the export

map name of VRF is the new configured name of route-map; if VRF is configured with a same name that export map, there will be a hint: "%Warning, This entry have been configed."

When using the command **no export map** ***WORD***, if the to be deleted export map name is not consistent with that of VRF, there will be a hint: "%Err, This entry is not configed"; if the to be deleted export map name is consistent with that of VRF, the export map of VRF will be deleted

When using the command **no export map**, the corresponding VRF is configured with export map and export map of VRF will be deleted; if the corresponding VRF is not configured with export map, there will be no response

MP-BGP route with VRF configured export map which sent out by VRF output target VPN expansion attribute

Example

The following example shows how to configure route-map name of VRF export map of PE as pe-export-map:

R1_config#ip vrf PE

R1_config_vrf_PE#export map pe-export-map

R1_config_vrf_PE#exit

R1_config#route-map pe-export-map 10 permit

R1_config_route_map #set extcommunity rt 1:1

Related command

ip vrf vrf-name

rd

57.4 import map

Syntax

To configure route-map filter condition of addting to VRF routing table, run the following command. To return to the default setting, use the no form of this command

import map *WORD*

no import map *WORD*

Parameter

WORD	Name of route-map

Default value

None

Command mode

VRF configuration mode

Usage guidelines

When using the command **import map** ***WORD***, if the corresponding VRF is not configured with import map, the **import** map name of VRF is that of route-map. If import map is configured with a different name, the import map name of VRF is the new configured name of route-map; if VRF is configured with a same name that import map, there will be a hint: "%Warning, This entry have been configed."

When using the command no **export map** ***WORD***, if the to be deleted import map name is not consistent with that of VRF, there will be a hint: "%Err, This entry is not configed"; if the to be deleted import map name is consistent with that of VRF, the import map of VRF will be deleted

When using the command **no export map**, the corresponding VRF is configured with import map and import map of VRF will be deleted; if the corresponding VRF is not configured with import map, there will be no response

MP-BGP route with VRF configured export map which sent out by VRF output target VPN expansion attribute

Example

The following example shows how to configure route-map name of VRF import map of PE as pe-export-map:

R1_config#ip vrf PE

R1_config_vrf_PE#import map pe-import-map

R1_config_vrf_PE#exit

R1_config#route-map pe-import-map 10 permit

R1_config_route_map # match ip address 1

R1_config_route_map #exit

R1_config#ip access-list standard 1

R1_config_std#permit 1.1.1.0 255.255.255.0

R1_config_std#exit

Related command

ip vrf vrf-name

rd

57.5 rd

Syntax

To configure VPN route tag of VRF, run the following command

rd *ASN:nn or IP-address:nn*

Parameter

ASN:nn or IP-address:nn	route tag of VPN

Default value

None

Command mode

VRF configuration mode

Usage guidelines

RD with 8-byte length is consist of 2-byte domain and 6-byte domain

The type domain determines the length of two sub-domains (manager domain and distribution value sub domain) in the value domain. At present, the type domain defines 3 values: 0, 1 and 2

For type 0, manger sub-domain has 2 bytes while the distribution value sub-domain has 4 bytes. Manger sub-domain uses 2-byte ASN and the distribution value domain offers value spaces managed by service provider. The value space is used for offering VPN service and is related to the distributed ASN

For type 1, manger sub-domain has 4 bytes while the distribution value sub-domain has 2 bytes. Manger sub-domain uses 1 IPv4 address and the distribution value domain offers value spaces managed by service provider. The value space is used for offering VPN service and is related to the distributed IPv4

For type 2, manger sub-domain has 4 bytes while the distribution value sub-domain has 2 bytes. Manger sub-domain uses ASN with 4 bytes and the distribution value domain offers value spaces managed by service provider. The value space is used for offering VPN service and is related to the distributed ASN

When using the command rd, if its corresponding VRF is configured with the same route tag, there is a hint: "%Warning, This entry have been configed"; if its corresponding VRF is configured with a different route tag, there is a hint: "%Warning, Do 'no ip vrf' before redefining the VRF". If you want to change the route tag of configured VRF, you must delete VRF first and re-create it; if the corresponding VRF hasn't configure the route tag, the route tag of VRF will become the new configured route tag

If configuring RD on PE router, it is not required all routes in one VPN use the same RD, but it must be guaranteed that each RD is globally exclusive

Example

The following example shows how to configure VPN route tag of VRF named PE to 1:1:

R1_config#ip vrf PE

R1_config_vrf_PE#rd 1:1

Related command

ip vrf vrf-name

57.6 route-target

Syntax

To configure target VPN expansion attribute, run the following command. To return to the default setting, use the no form of this command

route-target [export|import|both] *ASN:nn or IP-address:nn*

no route-target [export|import|both] *[ASN:nn or IP-address:nn]*

Parameter

ASN:nn or IP-address:nn	destination VPN expansion attribute

Default value

None

Command mode

VRF configuration mode

Usage guidelines

route-target ASN:nn or IP-address:nn

The command is used to add VRF input and output target VPN expansion attribute as the configured value

route-target export ASN:nn or IP-address:nn

The command is used to add VRF output target VPN expansion attribute as the configured value

route-target import ASN:nn or IP-address:nn

The command is used to add VRF input target VPN expansion attribute as the configured value

route-target both ASN:nn or IP-address:nn

The command is used to add VRF input and output target VPN expansion attribute as the configured value

no route-target

The command is used to delete all input and output target VPN expansion attribute of VRF

no route-target ASN:nn or IP-address:nn

The command is used to delete all input and output target VPN expansion attribute of VRF

The command is used to delete all output target VPN expansion attribute of VRF

no route-target export ASN:nn or IP-address:nn

The command is used to delete all output target VPN expansion attribute of VRF

no route-target import

The command is used to delete all output target VPN expansion attribute of VRF

no route-target import ASN:nn or IP-address:nn

The command is used to delete all input target VPN expansion attribute of VRF

The command is used to delete all output target VPN expansion attribute of VRF

no route-target both

The command is used to delete all output target VPN expansion attribute of VRF

no route-target both ASN:nn or IP-address:nn

The command is used to delete the designated input and output target VPN expansion attribute of VRF

The command route-target is used to configure route-target expansion attribute. If the target expansion attribute is existed, there is a hint: "%Warning, This entry have been configed."

The command no route-target is used to delete the command route-target expansion attribute. If the target expansion attribute is not existed, there is a hint: "%Err, This entry is not configed."

Using BGP expansion community attribute of BGP to limit issue of VPN routing information. The expansion community attribute works as the carrier of route attribute in BGP information

The route received by MP-BGP can only be added to VRF only if route-target import of VRF is allowed

When MP-BGP sending route, VRF configured route-target export taken as route-target expansion attribute of VPN route will be informed to other PE

Example

The following example shows how to input target VPN expansion attribute of VRF named PE as 1:1:

R1_config#ip vrf PE

R1_config_vrf_PE#route-target import 1:1

Related command

ip vrf vrf-name

rd

57.7 ip vrf forwarding

Syntax

To relate the interface to VRF, run the following command. To return to the default setting, use the no form of this command.

ip vrf forwarding *vrf-name*

no **ip vrf forwarding** *[vrf-name]*

Parameter

vrf-name	Name of VRF

Default value

The interface is non-related to VRF

Command mode

Interface configuration mode

Usage guidelines

ip vrf forwarding vrf-name

If the interface is not related to VRF, the command is used to relate the interface to VRF and delete IP address on the interface

If the interface is related to VRF, the command is used to delete the relation between the interface and the original VRF, set up the new relation between the interface and the new VRF, and delete the interface IP address

If the interface has been related to the same VRF, there is a hint: "%Warning, Interface type num have existed in VRF vrf-name." Here, type means the port type, num means the interface number, vrf-name means VRF name of the interface

no ip vrf forwarding

If the interface is not related to VRF, there is a hint: "%Warning, Interface type num not in any VRF." Here, type means the port type, num means the interface number

If the interface is related to VRF, delete the relation between the interface and VRF and IP address of the interface.

no ip vrf forwarding vrf-name

If there is no related VRF, there is a hint "Err, Interface type num not in VRF vrf-name." Here, type means the port type, num means the interface number, vrf-name means VRF name of the interface

If the interface is related to other VRF, delete the relation between the interface and VRF and IP address of the interface

Example

The following example shows how to configure the relation between interface VLAN 1 and VRF PE:

R1_config#ip vrf PE

R1_config_vrf_PE#rd 1:1

R1_config_vrf_PE#exit

R1_config #interface vlan 1

R1_config_v1#ip vrf forwarding PE

Related command

ip vrf vrf-name

57.8 ip vrf sitemap

Syntax

To configure MP-BGP forwarded routing and Soo attribute of network imbedded route, run the following command. To return to the default setting, use the no form of this command.

ip vrf sitemap *WORD*

no **ip vrf sitemap** *[WORD]*

Parameter

WORD	name of route-map

Default value

None

Command mode

Interface configuration mode

Usage guidelines

The interface which configures sitemap will influence MP-BGP forwarded route and Soo attribute of network

The command is configured with sitemap which will influence MP-BGP forwarded routing and Soo attribute of network imbedded route. There is no effect on ce route learned by MP-BGP

Example

The following example shows how to configure sitemap of vlan 1 to intf-sitemap:

R1_config #interface vlan 1

R1_config_v1#ip vrf sitemap intf-sitemap

R1_config_v1#exit

R1_config#route-map intf-sitemap 10 permit

R1_config_route_map #set extcommunity soo 1:1

Related command

ip vrf forwarding

57.9 show ip vrf

Syntax

To designate VRF information, run the following command

show ip vrf [brief|detail|interface] *[WORD]*

Parameter

WORD	name of VRF

Default value

None

Command mode

Other modes except exec

Usage guidelines

show ip vrf [vrf-name]

or

show ip vrf brief [vrf-name]

The command is used to show VRF brief information

show ip vrf detail [vrf-name]

The command is used to show details of VRF

show ip vrf interface [vrf-name]

The command is used to show port information of the designated VRF

Example

The following example shows how to show VRF information

R1 #show ip vrf

Name RD Interfaces

CE 1:1 vlan1

PE 2:1

Related command

ip vrf vrf-name

Chapter 58 Static Route Configuration Commands

58.1 ip route default

Syntax

To set the default route and the corresponding management distance, run **ip route default**. To cancel this settings, run **no** ip route default

ip route default {next-hop | interface} [distance] [tag tag] [global] [description]

no **ip route default** {next-hop | interface} [distance] [tag *tag*] [global]

Parameters

default	Sets the default route
next-hop	Means the next hop-IP address that is used to reach a network
interface	Stands for the to-be-used network interface
distance	Means the management distance (1-255), which is optional
tag tag	Sets a tag, which is used for matchup and route control
global	Next-hop address depends on the route in the global routing table
description	Means the description for the static routing items

Default Value

The function to generate a route is disabled

Command Mode

Routing configuration mode

Usage Guidelines

1.This command is used to set the static route which points towards a port or the next hop. In order to avoid route loopback, we make our devices not support the next-hop recursive research of the default route. The configured next hop must be the address of the next-hop device that directly connects the local port

2.The default route also supports to set the equivalent route

3.Parameters of global mode only can be used in VPN static route next hop in the global routing table

4.If a routing device has its default route configured and if the destination address of a packet cannot match up with a specific subnet route or a host route, the packet will be forwarded through the default route

5.If a route, which points to the loopback or null0 port, is set, it usually turns into a null route

6.The main routing table can contains up to 2K static routes

Example

The following example shows how to set a default route that points to next hop "192.168.1.133":

R-CE_config#interface vlan 1

R-CE_config_v1#ip address 192.168.1.132 255.255.255.0

R-CE_config_v1#exit

R-CE_config#ip route default 192.168.1.133

R-CE_config#

Related Command

ip route *A.B.C.D*

ip route vrf

58.2 ip route A.B.C.D

Syntax

To set a route and its management distance, run **ip route A.B.C.C mask**. To cancel this settings, run **no ip route default**

ip route *A.B.C.D mask* {next-hop | interface} [a.b.c.d] [distance] [tag *tag*] [global] [description]

no ip route A.B.C.D mask {next-hop | interface} [a.b.c.d] [distance] [tag tag] [global]

Parameters

A.B.C.D	Means the IP route of the destination address
mask	Stands for the mask of the destination address
next-hop	Means the next hop-IP address that is used to reach a network
interface	Stands for the to-be-used network interface
distance	Means the management distance (1-255), which is optional
a.b.c.d	Forwarding routing address
tag tag	Sets a tag, which is used for matchup and route control
global	Next-hop address depends on the route in the global routing table
description	Means the description for the static routing items

Default Value

The function to generate a route is disabled

Command Mode

Global configuration mode

Usage Guidelines

1.This command is used to set the static route which points towards a port or the next hop. In order to avoid route loopback, we make our devices not support the next-hop recursive research of the default route. The configured next hop must be the address of the next-hop device that directly connects the local port

2.The static route or default route also supports the equivalent route

3.Parameters of global mode only can be used in VPN static route next hop in the global routing table

4.If a routing device has its default route configured and if the destination address of a packet cannot match up with a specific subnet route or a host route, the packet will be forwarded through the default route

5.If a route, which points to the loopback or null0 port, is set, it usually turns into a null route

6.The main routing table can contains up to 2K static routes. The allowable maximum number of routes is 64K

Example

The following example shows how to set a static route that points to next hop "192.168.1.133":

R-CE_config#interface vlan 1

R-CE_config_v1#ip address 192.168.1.132 255.255.255.0

R-CE_config_v1#exit

R-CE_config#ip route 10.1.1.0 255.255.255.0 192.168.1.133

R-CE_config#

Related Command

ip route default

ip route vrf

58.3 ip route vrf

Syntax

To configure static route or default value route in vpn, and set the max routing capacity of VPN table, run the following command. To return to the default setting, use the no form of this command

ip route vrf *vpn_name* { {default | network mask } {next-hop | interface} [distance] [tag *tag*] [global] [description]} | **max-number** *value* }

no **ip route vrf** *vpn_name* {{default | network mask } {next-hop | interface} [distance] [tag *tag*] [global] [description]} | **max-number** *value*}

Parameter

vrf	Configure the default route in the corresponding VPN
vpn_name	name of the corresponding VPN
default	configure the default route
network	destination address IP route prefix
mask	destination address prefix mask
next-hop	next-hop IP address
interface	To be used network interface
distance	(optional) management distance (1 to 255)
tag tag	Set a tag, used for match and control the route
global	Next-hop address belongs to the route in the global routing table
description	Description of the static route entry
max-number	Configure the max route amount of VPN route entry
value	The max route amount of the routing table

Default value

No static route and default route

Command mode

Global configuration mode

Usage guidelines

1.The command is used to configure the static route designating port or next hop. For avoiding recursive query of the next-hop in the statix route, the next-hop configured must be next-hop device address of the directly connected local port

2.The static route or default route also supports configuration of the equivalent route

3.Parameters of global mode only can be used in VPN static route next hop in the global routing table

4.If the route configures a default route, once the packet destination address cannot be matched to the sub-net route or the host route, the packet will be forwarded by the default route

5.If it is configured with the route directing to loopback or Null0, it will become the black-hole route in general

6.The max routing number in VPN table is 10K

Example

The following example shows how to configure a static route directing to 192.168.1.133 in vpn_1:

R-CE_config#interface vlan 1

R-CE_config_vl1#ip vrf forward vpn_1

R-CE_config_v1#ip address 192.168.1.132 255.255.255.0

R-CE_config_v1#exit

R-CE_config#ip route vrf vpn_1 10.1.1.0 255.255.255.0 192.168.1.133

R-CE_config#

Related command

ip route default

ip route *A.B.C.D*

58.4 ip route bfd

Syntax

To enable the bidirectional link query of the static route, run the first one of the following two commands

ip route bfd { **static** { next-hop | A.B.C.D }| **query** <interval> | **reply** <interval> }

no ip route bfd { **static** { next-hop | A.B.C.D }| **query** <interval> | **reply** <interval> }

Parameters

Parameters	Description
static	Enables the bidirectional link query of the static route
next-hop	Enables the bidirectional link query of the static route which is urgent for network query
A.B.C.D	Means the address of the to-be-queried gateway
query	Sets the query interval
reply	Means the maximum interval between sending the query packets and receiving the response packets
interval	Means the configured interval

Default Value

The bidirectional link query of the static route is disabled

Command Mode

Global configuration mode

Usage Guidelines

None

Example

The following example shows hwo to detect the static routing gateway address 1.1.1.1:

ip route 10.0.0.0 255.0.0.0 1.1.1.1

ip route bfd static next-hop

ip route bfd static 1.1.1.1

Related Command

None

58.5 ip route load-balance

Syntax

To set the weight route balance, run the following command. To return to the default setting, use the no form of this command

ip route load-balance

no ip route load-balance

Parameters

None

Default Value

The load balance of the route is disabled and the route search is conducted according to the load balance of the equivalent route

Command Mode

Global configuration mode

Usage Guidelines

If you want the route load balance is conducted according to flows, you should run ip route load-balance in global configuration mode; moreover, you have to set the route load balance on the corresponding egress

Example

S 1.1.1.0/24 is directly connected, vlan 1

is directly connected, vlan 2

Supposed that the above-mentioned equivalent route exists and the following equivalent route needs to follow the ratio "2:3" to carry out the load balance, you should set as follows:

R1_config#ip route load-balance

R1_config#interface vlan 1

R1_config_v1#ip route-weight 2

R1_config_v1#exit

R1_config# interface vlan 2

R1_config_v2#ip route-weight 3

R1_config_v2#exit

Related Command

ip route-weight

58.6 ip route-weight

Syntax

To set the route weight based on the data flows on the egress port, run the first one of the following two commands

ip route-weight *value*

no ip route-weight

Parameters

Parameters	Description
value	Designates the route weight

Default Value

The route weight is not set by default, and if the equivalent route exists, the egress port need be selected according to the route balance mode

Command Mode

Interface configuration mode

Usage Guidelines

If ip route load-balance is not run, this command will not take effect during unicast flow forwarding even though the route weight is set on the interface

Example

S 1.1.1.0/24 is directly connected, vlan 1

is directly connected, vlan 2

Supposed that the above-mentioned equivalent route exists and the following equivalent route needs to follow the ratio "2:3" to carry out the load balance, you should set as follows:

R1_config#ip route load-balance

R1_config#interface vlan 1

R1_config_v1#ip route-weight 2

R1_config_v1#exit

R1_config#interface vlan 2

R1_config_v2#ip route-weight 3

R1_config_v2#

Related Command

ip route load-balance

58.7 ip route max-number

Syntax

To set the maximum number of routes, run the first one of the following two commands

ip route max-number *value*

no ip route max-number

Parameters

Parameters	Description
max-number	Sets the maximum number of routes for the global routing table
value	Means the maximum number of routes which is permitted by the routing table

Default Value

64K

Command Mode

Global configuration mode

Usage Guidelines

None

Example

The following example shows how to set the maximum number of routes in the global routing table to 20K.

R1_config#ip route max-number 20000

Related Command

None

58.8 ip route max-paths static

Syntax

To set the number of max next hop of the static equivalent route, run the following command. If there is no further settings, the default value is 8

ip route max-paths static *value*

no ip route max-number static

Parameters

Parameters	Description
value	The number of max next hop of the static equivalent route

Default Value

8

Command Mode

Global configuration mode

Usage Guidelines

None

Example

The following example shows how to set the number of max next hop of the static equivalent route to 5:

R1_config#ip route max-paths static 5

Related Command

None

58.9 show ip route

Syntax

To display the contents of the routing table according to users' requirements, run the following commands for different devices

show ip route [*A.B.C.D***| all | detail |** protocol **| bfd | summary | vrf** *vrf_name* **| information]**

Parameters

A.B.C.D	Displays a specific route. Displays all routes that can reach address A.B.C.D
all	Displays all routes, including those inactivated routes
cache	Displays the status of the route cache
summary	Displays the summary information about all activated routes
protocol	Means the protocol name or its keyword such as connected, static, bgp, Ospf, beigrp or rip

bfd	Means the bidirectional listening of the next hop of the static route
vrf	Displays the VPN route
vrf_name	Displays corresponding instance name of the VPN route
information	Displays the global route statistics information

Default Value

None

Command Mode

This command can be run in all modes except the EXEC mode

Usage Guidelines

None

Example

The following example shows how to display VPN_1 route:

show ip route vrf vpn_1

Related Command

show ip fib

58.10 show ip fib

Syntax

To display the route in the fast forwarding table, run the following command

show ip fib { route | vrf *vrf-name* **| summary }**

Parameters

Parameters	Description
route	Displays the route in the fast forwarding table
vrf vrf-name	Display the VRF route in the fast forwarding table
summary	Displays the statistics of FIB table

Default Value

None

Command Mode

This command can be run in all modes except the EXEC mode

Usage Guidelines

Summary, displays the statistics of FIB table, including the number of the total routing items, the number of the routing items, the status of synchronous traversing, the received number of added and deleted information sent by the main routing module

If there is a vpn route, this command will display the fast forwarding table of all vpn at the same time

Example

None

Related Command

show ip route

58.11 debug ip routing

Syntax

Stand-alone routing (including distributed main control terminal) device debugging commands:

debug ip routing { bfd | memory | message | search | timer | cache | vrf *vrf_name* }

Parameters

Parameters	Description
bfd	Means the debugging information about the BFD link of the static route.
memory	Means the debugging information about memory allocation.
message	Means the debugging information about route addition and deletion.
search	Means the debugging information about route query.
timer	Means the debugging information about the timer timeout.
cache	Means the debugging information about cache change.
vrf vrf-name	Means to specify vrf

Default Value

No debugging information is exported

Command Mode

EXEC

Usage Guidelines

To disable the debugging information, you should run no debug ip routing

Example

None

Related Command

None

Chapter 59 RIP Configuration Commands

59.1 auto-summary

Syntax

To activate the automatic summarization function, use the auto-summary command. To turn off this function, use the no form of this command

auto-summary

no auto-summary

Parameter

This command has no parameter or keywords

Default value

Enabled by default

Command mode

RIP global configuration

Usage guidelines

Routing summarization reduces the amount of routing information in the routing tables and switching information. Routing Information Protocol(RIP) do not support subnet mask, therefore, if it is forwarded to subnets, routing possibly cause ambiguity. RIP Version 1 always uses routing summarizarion. If using RIP Version 2, you can turn off routing summarization by using the **no auto-summary** command. When routing summarization is off, subnets are advertised

Example

To specify RIP version on Serial 1/0 as RIP Version 2 and turn off routing summarization function

router rip 1

version 2

no auto-summary

Related commands

version

59.2 default-information originate

Syntax

To generate a default route, use the default-information originate command. To disable this function , use the no form of this command

default-information { originate | originate-safe }

no default-information

Parameter

originate: Generates a default route in the RIP local routing table without condition

originate-safe: Generates RIP local default route when there is non-RIP default routes in the master routing table

Default

Disable this function by default

Command mode

RIP Global configuration mode

Usage guidelines

After the default-information originate command is activated, the routing information(0.0.0.0/0) is accompanied when send routing updating

Example

When send routing updating information, the default routing(0.0.0.0/0) is accompanied

!

router rip 1

version 2

default-information originate

!

ip route default vlan1

!

59.3 default-metric

To set default metric values for import routing, use the default-metric command. To return the default stata, use the no form of this command

default-metric *number*

no default-metric

Parameter

parameter	description
number	Default metric value. It has a value from 1 to 16

Default value

1

Command mode

RIP Global configuration mode

Usage guidelines

The default-metric command is used to set default routing metric used in importing routing of other routing protocols into Rip packets. When import routing of other protocols, use the specified default routing by default-metric if no specified routing metric

Example

The following example shows a routing switch in autonomous system 119 using both the RIP and the OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the OSPF-derived routes a RIP metric of 8

router rip 1

default-metric 8

redistribute ospf 119

Related commands

redistribute

default-information

59.4 ip rip authentication

Syntax

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the **ip rip authentication** command in interface configuration mode. To restore plain text authentication, use the no form of this command

ip rip authentication {**simple** | **message-digest**}

no ip rip authentication

Parameter

parameter	description
simple	Plain text authentication.
Md5	MD5 ciphertext authentication type
Dynamic	Dynamic authentication type
Commit	Send authentication request immediately (used for immediate re-authentication after authentication configuration changes)

Default value

Disabled

Command mode

Interface configuration mode

Usage guidelines

RIP Version 1 does not support authentication

Example

The following example configures the interface to use MD5 ciphertext authentication type:

ip rip authentication md5;

Configure interface to use dynamic ciphertext authentication:

Ip rip authentication dynamic

Related commands

ip rip password

ip rip message-digest-key

59.5 ip rip md5-key

Syntax

To activate authentication for RIP-2 packet and designate MD5-key ciphertext on the interface, run the following command. To return to the default setting, use the no form of this command

ip rip md5-key *key-id* **md5** [0 | 7] *password*

no ip rip md5-key

Parameter

Parameter	Description
key-id	An identifier
Password	A designated password
0	The key is plaintext (default value)
7	The key is ciphertext

Default value

Invalid MD5 authentication

Command mode

Interface configuration mode

Usage guidelines

If there is no configuration of **ip rip md5-key key-id md5 password**, there will be no authentication

Example

The following example shows how to configure MD5 encrypt authentication packet which belongs to mykey

ip rip md5-key 4 md5 mykey

Related command

ip rip authentication

59.6 ip rip dynamic-key

Syntax

To activate authentication of RIP-2 and designate MD5 or SHA1 ciphertext authentication key, run the following command. To return to the default setting, use the no form of this command

ip rip dynamic-key *key-id* {**md5|sha1**} [0 | 7] *password xxxx-xx-xx-xx:xx xx:xx*

no ip rip dynamic-key *key-id* {**md5|sha1**}

Parameter

Parameter	Description
key-id	1 identifier
{md5|sha1}	Algorithm of key corresponding to key id
[0 | 7]	Designate the key type: plaintext (0) or ciphertext (7)
Password	Designate keyword (20 bytes in maximum)
xxxx-xx-xx-xx:xx	Effective time of key corresponding to key id
xx:xx	Effective time length of key corresponding to key id

Default value

Disabled dynamic authentication

Command mode

Interface configuration mode

Usage guidelines

Generally speaking, every key is effective only in the effective time period (As its effective time is based on the system time, it is suggested that the interface neighbor time must be consistant, for instance, refer to a standard time)

If the dynamic authentication is enabled and no key is activated, only non-authenticated packet can pass the authentication

If period of validity of key is overtime, No key can be updated, the length of effective time of the last key can be automatically extended, until the new key takes effect

You can add many keys one time, the system will takes effect and lose effect according to configuration of the key

It enables many keys taking effect. You can choose one key to execute operations when forwarding packets and verify the packet according to key id after receiving the packet

Suggestion: The effective time length of every key is 24 hours and the one key in operation is activated and the effective time of one key is three minutes before the effective time of last key

Example

ip rip dynamic-key 2 sha1 xxxxxxxxxx 2009-3-3-9:0 24:5

ip rip dynamic-key 5 md5 xxxxxxxxx 2009-3-10-9:0 24:5

ip rip dynamic-key 6 sha1 xxxxxxxxxxxx 2009-3-11-9:0 24:5

.

.

Related command

ip rip authentication

59.7 ip rip password

Syntax

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify the plain text authentication used on the interface, use the **ip rip password** command. Use the no form of this command to prevent authentication

ip rip password *password*

no ip rip password

Parameter

parameter	description
password	The specified password

Default value

No authenctication

Command mode

Interface configuration mode

Usage guidelines

No authentications are carried out on interface without using the **ip rip password** command to configure any password

Example

The following example configures interface to receive and send any plain text authentication packet that belong to password 'mykey'.

ip rip password mykey

Related commands

ip rip authentication

59.8 ip rip passive

Syntax

To cancel the routing switch to send routing updating on interface, use the **ip rip passive** command. To reactivate the routing updating, use the no form of this command

ip rip passive

no ip rip passive

Parameter

None

Default value

Send routing updates on the interface

Command mode

Interface configuration mode

Usage guidelines

If you cancel routing updating on a certain interface, a specified subnetwork will keep on announcing to other interfaces, and the routing updating that from other routing switches can be continuedly accepted and dealt with on this interface

Example

The following example sends RIP packets updating to all interfaces (except for VLAN1) that enable RIP process 1:

interface vlan1

ip rip 1 enable

ip address 172.15.0.1 255.255.0.0

ip rip passive

router rip 1

Related commands

None

59.9 ip rip deaf

Syntax

To disable receiving rip protocol packet on the interface, run the following command. To return to the default setting, use the no form of this command

ip rip deaf

no ip rip deaf

Parameter

None

Default value

Disabled

Command mode

Interface configuration mode

Usage guidelines

If the **ip rip deaf** command is used on one interface, it will continue to forward routing requirements outward and inform the routing update, but without accepting any rip protocol packet

Example

The following example shows how to forward RIP packets update to vlan 1 but not receiving rip packets:

interface vlan1

ip rip 1 enable

ip address 172.16.0.1 255.255.0.0

ip rip deaf

router rip 1

Related command

None

59.10 ip rip receive version

Syntax

To specify a Routing Information Protocol (RIP) version to receive on specified interface, use the **ip rip receive version** command in interface configuration mode. To follow the global version rules, use the no form of this command

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter

parameter	description
1	(Optional) Accepts only RIP Version 1 packets on the interface.
2	(Optional) Accepts only RIP Version 2 packets on the interface.

Default value

Accepts RIP Version 1 and RIP Version 2 packets

Command mode

Interface configuration mode

Usage guidelines

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured. You can configure the interface to receive both RIP versions

Example

The following example configures the interface to receive both RIP Version 1 and Version 2 packets:

ip rip receive version 1 2

The following example configures the interface to receive only RIP Version 1 packets:

ip rip receive version 1

Related commands

ip rip send version

version

59.11 ip rip send version

Syntax

To specify a Routing Information Protocol (RIP) version to send on specified interface, use the **ip rip send version** command in interface configuration mode. To follow the global version rules, use the no form of this command

ip rip send version [**1** | **2** | **compatibility**]

no ip rip send version

Parameter

parameter	description
1	(Optional) Sends only RIP Version 1 packets out the interface
2	(Optional) Sends only RIP Version 2 packets out the interface

compatibility	(Optional) Broadcasts only RIP Version 2 packets out the interface

Default value

If there is no configured global version and there is no peer or if version cannot be determined according to rip's adaptive rules, only RIP-2 packets are send

Command mode

Interface configuration mode

Usage guidelines

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured

Example

The following example configures the interface to send only RIP Version 1 packets out the interface:

ip rip send version 1

The following example configures the interface to send only RIP Version 2 packets out the interface:

ip rip send version 2

Related commands

ip rip receive version

version

59.12 ip rip v1demand

Syntax

To forward request packets with v1 format, run the following command. To return to the default setting, use the no form of this command

ip rip v1demand

no ip rip v1demand

Parameter

None

Default value

The command follows the set global version and interface version. If neither, it will follows the auto-adaptation principle (based on the received opposite terminal)

Command mode

Interface configuration mode

Usage guidelines

The command is used to forward request packets with v1 format. The command is non-related to version in the

global mode and the version on the interface. The command is only used in forwarding request. In the normal condition, the interface and the global configuration modes are applied (such as update packet)

Example

The following example shows how to configure request packets with v1 format and RIP updated packets with v2 format:

ip rip v1demand

ip rip send version 2

Related command

Ip rip v2demand

Ip rip send

Version

59.13 ip rip v2demand

Syntax

To forward request packets with v2 format, run the **ip rip v2demand** command. To return to the default setting, use the **no ip rip v2demand** or **default ip rip v2demand** command

ip rip v2demand

no ip rip v2demand

Parameter

None

Default value

The command follows the set global version and interface version. If neither, it will follow the auto-adaptation principle (based on the received opposite terminal)

Command mode

Interface configuration mode

Usage guidelines

The command is used to forward request packets with v2 format. The command is non-related to version in the global mode and the version on the interface. The command is only used in forwarding request. In the normal condition, the interface and the global configuration modes are applied (such as update packet)

Example

The following example shows how to configure request packets with v2 format and RIP updated packets with v1 format:

ip rip v2demand

ip rip send version 1

Related command

Ip rip v1demand

Ip rip send

version

59.14 ip rip split-horizon

Syntax

To enable the split horizon mechanism, use the **ip rip split-horizon** command in interface configuration mode. To disable the split horizon mechanism, use the no form of this command

ip rip split-horizon {simple | poisoned}

no ip rip split-horizon {simple | poisoned}

Parameter

Parameter	Description
simple	Simple split horizon
poisoned	Split horizon with poisoned reversal

Default value

Default behavior varies with media type

Command mode

Interface configuration mode

Usage guidelines

For all interfaces except those for which either Frame Relay or Switched Multimegabit Data Service (SMDS) encapsulation is enabled, the default condition for this command is **ip split-horizon**; in other words, the split horizon feature is active. If the interface configuration includes encapsulation frame-relay, then the default is for split horizon to be disabled

Note: For networks that include links over X.25 packet switched networks (PSNs), the neighbor routing switch configuration command can be used to defeat the split horizon feature. You can as an alternative explicitly specify the **no ip rip split-horizon {simple | poisoned}** command in your configuration. However, if you do so you must similarly disable split horizon for all routing switches in any relevant multicast groups on that network

If split horizon has been disabled on an interface and you want to enable it, use the **ip rip split-horizon {simple | poisoned}** command to restore the split horizon mechanism

Note: In general, changing the state of the default for the **ip rip split-horizon {simple | poisoned}** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a PSN), you must disable split horizon for all routing switches and access servers in any relevant multicast groups on that network

Example

The following simple example disables split horizon on vlan1

interface vlan1

no ip rip split-horizon simple

Related commands

neighbor

59.15 ip rip process-id enable

Syntax

To set the interface relate to one RIP instance, run the following command. To return to the default setting, use the no form of this command

ip rip *process-id* **enable**

no ip rip *process-id* **enable**

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535

Default value

None

Command mode

Interface configuration mode

Usage guidelines

When one interface is configured with this command, the interface will be binded to its corresponding rip instance, becoming rip interface of the instance and generates the direct network segment corresponding to the interface as the rip route; every interface can only connect to one RIP instance. By default the interface does not relate to any instance

Note: If enable one to be created RIP instance on the interface, create RIP instance with the instance number and vrf of the interface; if enable an existed instance on the interface, but the port binded vrif and the designated vrf when creating the instance, the interface will not become the activation interface of RIP, until the interface vrf is consistant with the instance designated vrf

Example

interface vlan1

ip rip 1 enable

Related command

Router rip ***process-id*** [vrf ***name***]

59.16 neighbor

Syntax

To define a neighboring routing switch with which to exchange routing information, use the **neighbor** command in routing switch configuration mode. To remove an entry, use the no form of this command

neighbor *ip-address*

no neighbor *ip-address*

Parameter

parameter	description
ip-address	IP address of a peer routing switch with which routing information will be exchanged

Default value

No neighboring routing switches are defined

Command mode

RIP Global configuration mode

Usage guidelines

This command permits the point-to-point (nonbroadcast) exchange of routing information in order to meet special requirements of the specified nonbroadcast network

Example

In the following example, the neighbor routing switch configuration command permits the sending of routing updating to specific neighbors

router rip 1

neighbor 131.108.20.4

Related commands

Router rip ***process-id***

59.17 offset

Syntax

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the **offset** command in routing switch configuration mode. To remove an offset list, use the no form of this command

offset {*type number* | *****} {**in | out**} *access-list-name offset_value*

no offset {*type number* | *****} {**in | out**}

Parameter

parameter	description
In	Applies the access list to incoming metrics
Out	Applies the access list to outgoing metrics
access-list-name	Standard access list number to be applied
Offset_value	Positive offset to be applied to metrics for networks matching the access list
type	(Optional) Interface type to which the offset list is applied
number	(Optional) Interface number to which the offset list is applied

Default value

This command is disabled by default

Command mode

RIP Global configuration mode

Usage guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric

Example

In the following example, the routing switch applies an offset of 10 to routes learned from VLAN1 that satisfies the access list abc:

offset vlan1 in abc 10

59.18 router rip process-id

Syntax

To configure RIP instance in the global mode, run the following command. To return to the default setting, use the no form of this command

router rip *process-id* [vrf *vrf-name*]

no router rip *process-id* [vrf *vrf-name*]

Parameter

Parameter	Description
Process-id	Configures instance ID. The value ranges from 1 to 65535

Vrf-name	Specify the VRF to which the RIP instance belongs

Default value

By default no RIP instance is operated. When configuring instance, process id is not by default

Command mode

Global configuration mode

Usage guidelines

Only RIP instance is enabled can the routing instance configuration mode is entered and all global configuration parameters of RIP instance can be configured. Configuration of parameters related to the interface does not limit to the enable of RIP instance

Example

The following example shows how to enable RIP instance and enter the instance configuration mode.

router rip 1

Related command

ip rip *process-id* **enable**

59.19 timers expire

Syntax

To adjust RIP network timers, use the **timers expire** configuration command. To restore the default timers, use the no form of this command

timers expire *interval*

no timers expire

Parameter

parameter	description
interval	Interval of time in seconds after which a route is declared invalid; it should be at least three times the value of update. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds

Default value

180 seconds

Command mode

RIP global configuration mode

Usage guidelines

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network

Note: The current and default timer values can be seen by the show ip rip command

Example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable

router rip 1

timers expire 30

59.20 timers holddown

Syntax

To adjust RIP network timers, use the **timers holddown** configuration command. To restore the default timers, use the no form of this command

timers holddown *second*

no timers holddown

Parameter

parameter	description
second	Interval in seconds during which routing information regarding better paths is suppressed. It should be at least three times the value of update. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 120 seconds

Default value

120 seconds

Command mode

RIP global configuration mode

Usage guidelines

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network

Note: The current and default timer values can be seen by the show ip rip command

Example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable

router rip 1

timers holddown 30

59.21 timers update

Syntax

To adjust RIP network timers, use the **timers update** command. To restore the default timers, use the no form of this command

timers update update

no timers update

Parameter

parameter	description
update	Rate in seconds at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds

Default value

30 seconds

Command mode

RIP global configuration mode

Usage guidelines

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network

Note: The current and default timer values can be seen by the show ip rip protocol command

Example

In the following example, updates are broadcast every 5 seconds

router rip 1

timers update 5

Note that by setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a big concern on faster-speed serial lines. Also, if you have many routes in your updates, you can cause the routing switches to spend an excessive amount of time processing updates

59.22 timers trigger

Syntax

To adjust trigger update timer, run the following command. To return to the default setting, use the no form of this command

timers trigger *second*

no timers trigger

Parameter

Parameter	Description
second	Time interval of trigger update (unit: s)

Default value

5s

Command mode

RIP Global configuration mode

Usage guidelines

The basic timer parameters of RIP can be adjusted. As RIP works on the asynchronous routing algorithm, it's important to set timer parameters of the routers and access routers in the network to the same

Note:The show ip rip command is used to show parameters of the current or default timer.

Example

router rip 1

timers trigger 4

59.23 timers peer

Syntax

To adjust peer overtime timer of RIP network, run the following command. To return to the default setting, use the no form of this command

timers peer *second*

no timers peer

Parameter

Parameter	Description

second	Time interval of peer overtime

Default value

102s

Command mode

RIP Global configuration mode

Usage guidelines

The basic timer parameters of RIP can be adjusted. As RIP works on the asynchronous routing algorithm, it's important to set timer parameters of the routers and access routers in the network to the same

Note: The show ip rip protocol command is used to show parameters of the current or default timer

Example

router rip 1

timers peer 50

59.24 validate-update-source

Syntax

To have the software validate the source IP address of incoming routing updates for RIP routing protocols, use the **validate-update-source** configuration command. To disable this function, use the no form of this command

validate-update-source

no validate-update-source

Parameter

This command has no parameters or keywords

Default value

Enabled

Command mode

RIP global configuration mode

Usage guidelines

This command is only applicable to RIP and IGRP. The software ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface

Disabling split horizon on the incoming interface will also cause the system to perform this validation check

For unnumbered IP interfaces (interfaces configured as ip unnumbered), no checking is performed

Example

router rip 1

no validate-update-source

59.25 check-zero-domain

Syntax

To check the legality of zero-domain in the routing entries receiving from the neighbor, run the following command. To return to the default setting, use the no form of this command

check-zero-domain

no check-zero-domain

Parameter

No parameters or key words

Default value

Activated

Command mode

RIP Global configuration mode

Usage guidelines

The command is mainly used in version 1. Only the segments such as route-tag, subnet mask and next hop of the routing entries received in version 1 must be 0

Example

router rip 1

no check-zero-domain

59.26 version

Syntax

To specify a RIP version used globally by the routing switch, use the version routing switch configuration command. Use the no form of this command to restore the default value

version {1 | 2}

no version

Parameter

parameter	description
1	Specifies RIP Version 1
2	Specifies RIP Version 2

Default value

Send and receive rip packets according to the configuration on each port. If no version is configured on the port, select the version of peer according to the rip adaptive rules. If no peer is configured on the port, the default RIP-2 packets are sent

Command mode

RIP global configuration mode

Usage guidelines

To specify RIP versions used on an interface basis, use the **ip rip receive version** and **ip rip send version** commands; or it will send RIP packets in terms of the global configuration version

Example

The following example enables the software to send and receive RIP Version 2 packets:

version 2

Related commands

ip rip receive version

ip rip send version

59.27 distance

To define an administrative distance for RIP routes, use the **distance** command in routing switch configuration mode

distance weight [*address mask* [*access-list-name*]]

no distance weight [*address mask* [*access-list-name*]]

Parameter

parameter	description
weight	Administrative distance. An integer from 1 to 255. It is recommended to use 10 to 255. (The values 0 to 9 are reserved for internal use.) Routes with a distance value of 255 are not installed in the routing table.)
address	(Optional) Source IP address (in four-part, dotted decimal notation)
mask	(Optional) IP address mask (in four-part, dotted decimal notation) If a certain digit is 0, software will omit the corresponding value in the address
access-list-name	(Optional) Named access list to be applied to incoming routing updates

Default value

120

Command mode

RIP global configuration mode

Usage guidelines

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. When the optional access list name or number is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the routing switch that supplies the routing information

Example

The following example sets the administrative distance to 100 for the routing switch with the address 192.1.1.0/24

router rip 1

distance 100 192.1.1.0 255.255.255.0

59.28 filter

Syntax

To filter for RIP routes, use the filter command

filter { *type number* | * } { **in** | **out** } { **access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name* }

no filter { *type number* | * } { **in** | **out** } [**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*]

Parameter

parameter	description
access-list-name	Standard IP access list name. This list defines networks of which are received or suppressed in routing update
prefix-list-name	Standard IP prefix list name. This list defines networks of which are received or suppressed in routing update
in/out	Applies access list for in/out routing update
type	(Optional) Interface type
number	(Optional) Indicates number of interface on which applies the access list for in/out routing update. If no interface is defined, the access list is applicabale to all in/out routing update

Default value

Disabled

Command mode

RIP global configuration mode

Usage guidelines

Filter the route that are to be sent and received.If you use the access-list command to configure access list for dynamic routing protocol, you shoul use the standard access list

example

The following example filter route 10.0.0.0/8 from vlan1:

router rip 1

filter vlan1 out access-list mylist

ip access-list standard mylist

deny 10.0.0.0 255.0.0.0

permit all

59.29 maxinum-nexthop

Syntax

To configure the max equivalent routing number in RIP routing information, run the following command. To return to the default setting, use the no form of this command

maximum-nexthop *number*

no maximum-nexthop

Parameter

Parameter	Description
number	The max equivalent routing number. The value ranges from 1 to 16.

Default value

4

Command mode

RIP Global configuration mode

Usage guidelines

The command is used to set the max equivalent routing number. When learning the complete equivalent routing information (metric, distance) from many neighbors. If the number of neighbor is greater than the max value of the equivalent routing number, there will be no next hop adding to the routing table

Example

The following example shows how to the equivalent routing number of RIP routing information is 5

router rip 1

maximum-nexthop 5

Related command

None

59.30 input-queue

Syntax

To adjust the size of receiving queue, run the following command. To return to the default setting, use the no form of this command

input-queue *number*

no input-queue

Parameter

Parameter	Description
number	Size of the receiving queue. The value ranges from 1 to 61440

Default value

200

Command mode

Global configuration mode

Usage guidelines

The command is used to set size of the receiving queue which unit is packet. The size is suggested not to oversmall, otherwise, the routing cannot not be fully learned when quantities of routing are imput

Example

The following example shows how to set the size of receiving queue of RIP routing information to 500.

router rip 1

input-queue 500

Related command

None

59.31 show ip rip

Syntax

To display RIP main information, use the show ip rip command

show ip rip

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

User can see the current configuration status about RIP instances.according to the output of this command

Example

The following example displays configuration parameter information about RIP:

Switch#show ip rip

Process: 2

Update: 30, Expire: 180, Holddown: 120

Input-queue: 50

Validate-update-source: Enable

zero-domain-check: Enable

Neighbor List:

interface List:

interface Loopback0

Description of the displaying fields:

Field	Description
Process	Configure instance ID
Update	Interval of time at which updates are sent.
Holddown	Interval (in seconds) during which routing information regarding better paths is suppressed.
Expire	Interval of time after which a route is expired.
Input-queue	Message queue depth
Validate-update-source	Check the validity of the source address.
zero-domain-check	Check the validity of message domain.
Neighbor List	Configure the Neighbor list.

interface List	List of ports associated with the instance

59.32 show ip rip process-id interface

Syntax

To show all interfaces of RIP instances and status of these interfaces, use the following command

show ip rip *process-id* interface

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show all interfaces of RIP instances and status of these interfaces

Example

The following example shows how to show all interfaces of RIP instances and status of these interfaces

```
Switch_config#show ip rip 1 interface
Interface Loopback7 ,vrf (0)
  Address:22.2.2.2, mask:255.255.255.0
  state:active
  Send version: V1(default)
  Receive version: V1 and V2(default)
  Passive: Disable
  v1demand: Disable
  v2demand: Disable
  deaf: Disable
```

Authentication type: NULL

MD5 authentication key: NULL

Simple password: NULL

Interface GigaEthernet0/0 ,vrf (0)

Address:2.2.2.1, mask:255.255.255.0

state:active

Send version: V1(default)

Receive version: V1 and V2(default)

Passive: Disable

v1demand: Disable

v2demand: Disable

deaf: Disable

Authentication type: simple

MD5 authentication key: NULL

Simple password: NULL

59.33 show ip rip process-id summary

Syntax

To show statistics of all routes of RIP instances, run the following command. To return to the default setting, use the no form of this command

show ip rip *process-id* summary

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information, and show the designated statistics of all routes of RIP instances

Example

The following example shows how to show statistics of all routes of RIP instances

Switch_config#show ip rip 1 summary

------------------- RIP Process 1 Summary Statistic ------------------

RIP route table:

Maximum route number :1024

Total route number :8

Connect route number :2

Learn route number :4

Redistributed route number :0

Holddown route number :0

--

59.34 show ip rip process-id database

Syntax

To show all route information of RIP instances, run the following command

show ip rip *process-id* database

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information. It shows all routing information of RIP

Example

The following example shows how to show all routing information o RIP

Switch#show ip rip process-id database

1.0.0.0/8 auto-summary

1.1.1.0/24 directly connected Loopback1

100.0.0.0/8 via 192.1.1.2 (on Vlan1)

192.1.1.0/24 redistributed

Definitions of the above domains:

Domain	Description
Network-number/network-mask	RIP routing
Summary/connected/redistributed/ via gateway	The corresponding RIP route type
interface	Ports corresponding to RIP route

59.35 show ip rip process-id protocol

Syntax

To show RIP configuration information, run the following command

show ip rip *process-id* **protocol**

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the current RIP configuration information

Example

The following example shows how to show the configuration information of RIP protocol

Switch_config_rip_1#show ip rip 1 pr

RIP 1 is Active

update interval 30(s), Invalid interval 180(s)

Holddown interval 120(s), Trigger interval 1(s), peer interval 102(s)

Automatic network summarization: Enable

Filter list:

Offset list:

Redistribute policy:

Interface send version and receive version:

Global version : default

Interface Send-version Recv-version Nbr_number

Loopback7 V2 V1 V2 0

GigaEthernet0/0 V2 V1 V2 4

Distance: 0 (default is 120):

Maximum route count: 1024, Current route count:8

59.36 show ip rip process-id peer

Syntax

To show status information of RIP neighbor, run the following command

show ip rip *process-id* **peer**

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the current status information of RIP neighbor to the user

59.37 debug ip rip database

Syntax

To monitor RIP route event, run the following command

debug ip rip database

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the event of current RIP route

Example

The following example shows how to monitor the event of RIP route.

switch# debug ip rip database

RIP-DB: Adding 192.1.1.0/24 <metric 2> via 10.1.1.2 to RIP database

Definitions of the above domains:

Domain	Description
192.1.1.0/24	Route adding to the routing table
<metric 2>	Routing metric value
10.1.1.2	Gateway address of the learned route

59.38 debug ip rip packet [send | receive]

Syntax

To monitor packets RIP received, run the following command

debug ip rip packet

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the received and sent packets of the current RIP to the user

Example

The following example shows how to monitor packets of RIP:

Switch# debug ip rip packet

RIP: send to 255.255.255.255 via Loopback1

vers 1, CMD_RESPONSE, length 24

192.1.1.0/0 via 0.0.0.0 metric 2

When running version 2, the following will be output:

RIP: send to 224.0.0.9 via Loopback1

vers 2, CMD_RESPONSE, length 24

192.1.1.0/24 via 0.0.0.0 metric 2

RIP: recv RIP from 10.1.1.2 on Vlan1

vers 2, CMD_REQUEST, length 24

Definitions of the above domains:

Domain	Description
Send/Recv	Packets forwarded(send) and received
to/from xx.xx.xx.xx	Destination address or source address of IP packets
via Loopback1/on Vlan1	Ports for sending or receiving packets
vers 2	Version numbers for sending or receiving packets
CMD_RESPONSE/ CMD_REQUEST	Packet type
length 24	Packet length
192.1.1.0/24	Destination network of the routing information
via 0.0.0.0	Next hop address
metric	Metric of the route

59.39 debug ip rip message

Syntax

To monitor RIP events, run the following command

debug ip rip message

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show users to events of the current RIP, such as port address, status change and timer overtime

Example

The following example shows how to monitor RIP packets:

Switch# debug ip rip message

RIP: Update timer timeout(process 1)

Chapter 60 BEIGRP Configuration Commands

60.1 auto-summary

Syntax

The auto summary is disabled by default. Since auto summary is currently not supported to enable, this command has no form only

no auto-summary

Parameter

None

default

Disabled

Command mode

Router configuration

Usage guidelines

None

related commands

None

60.2 clear ip beigrp neighbors

Syntax

To delete entries from the neighbor table, use the **clear ip beigrp** command in EXEC mode

clear ip beigrp [*as-number*] **neighbors** [*ip-address* | *interface*-type *interface-number*]

Parameter

parameter	description
as_number	(Optional) Neighbor's autonomous system number
ip-address	(Optional) Address of BEIGRP's neighbor
interface	(Optional) Interface name. After typing this parameter, all neighbors on this interface will perform adjacent reset

default

none

Command mode

EXEC

Usage guidelines

All BEIGRP's neighbors will be reset without specifying any parameter

The use of this command will lead adjacent reset of one or several neighbors, and then triggers routing operation. In the case when many routes are influenced, it may cause route fluctuation, and it needs some time to convergence again. So we recommend not to use this command unless the system is in the network debugging stage

Example

The following example removes all neighbors on vlan 1 and triggers recalculation of the related routes:

clear ip beigrp neighbors vlan 1

60.3 debug ip beigrp

Syntax

To trace BEIGRP protocol information, you can press this command in the privileged EXEC mode

debug ip beigrp

no debug ip beigrp

parameter

none

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command

Example

debug ip beigrp

60.4 debug ip beigrp fsm

Syntax

To trace the change of state machine of BEIGRP DUAL algorithm, use the debug ip beigrp fsm command in EXEC command

debug ip beigrp fsm

Parameter

none

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command

Related commands

debug ip beigrp packets

60.5 debug ip beigrp neighbors

Syntax

To display the establishment and deletion of BEIGRP neighbors, use the debug ip beigrp neighbors command in EXEC mode

debug ip beigrp neighbors

Parameter

None

Default

None

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command

example

TestC#debug ip beigrp neighbors

BEIGRP: Neighbor 192.168.20.141 went down on vlan 1 for peer restarted.

BEIGRP: Neighbor(192.168.20.141) not yet found.

BEIGRP: Neighbor(192.168.20.141) not yet found.

BEIGRP: New neighbor 192.168.20.141

BEIGRP: Neighbor 202.117.80.143 went down on vlan 2 for manually cleared.

BEIGRP: Neighbor 192.168.20.141 went down on vlan 1 for manually cleared.

BEIGRP: New neighbor 192.168.20.204

BEIGRP: New neighbor 202.117.80.143

BEIGRP: New neighbor 192.168.20.141

related commands

debug ip beigrp fsm

debug ip beigrp packet

Syntax

To display BEIGRP packets situations, use the debug ip beigrp packet command in EXEC mode

debug ip beigrp packets [ack | hello | query | reply | retry | terse | update | error]

no debug ip beigrp packets [ack | hello | query | reply | retry | terse | update | error]

Parameter

parameter	description
ack	(Optional) Traces ACK pacekts
hello	(Optional) Traces hello packets
query	(Optional) Traces query packets
reply	(Optional) Traces reply packets
retry	(Optional) Traces retry packets
terse	(Optional) Traces all packets except hello packets
update	(Optional) Traces update packets
error	(Optional) Traces error packets

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command

example

router#debug ip beigrp packet

BEIGRP: Send HELLO packet to 224.0.0.10 via vlan 2 with Ack 0/0

BEIGRP: Receive ACK packet from 192.168.20.141 via vlan 1 with Ack 0/54

BEIGRP: Receive HELLO packet from 202.117.80.143 via vlan 2 with Ack 0/0

BEIGRP: Receive UPDATE packet from 192.168.20.204 via vlan 1 with Ack 142/0

BEIGRP: Send HELLO packet to 192.168.20.204 via vlan 1 with Ack 0/142

BEIGRP: Receive HELLO packet from 192.168.20.141 via vlan 1 with Ack 0/0

BEIGRP: Receive HELLO packet from 192.168.20.204 via vlan 1 with Ack 0/0

BEIGRP: Receive QUERY packet from 192.168.20.204 via vlan 1 with Ack 143/0

BEIGRP: Send HELLO packet to 192.168.20.204 via vlan 1 with Ack 0/143

BEIGRP: Send REPLY packet to 192.168.20.204 via vlan 1 with Ack 55/143

BEIGRP: Send UPDATE packet to 224.0.0.10 via vlan 2 with Ack 57/0

BEIGRP: Receive ACK packet from 192.168.20.204 via vlan 1 with Ack 0/55

BEIGRP: resend UPDATE packet for neighbor 192.168.20.204 with retry num 1.

BEIGRP: Receive ACK packet from 202.117.80.143 via vlan 2 with Ack 0/57

BEIGRP: Send UPDATE packet to 202.117.80.143 via vlan 2 with Ack 57/77

BEIGRP: Send UPDATE packet to 224.0.0.10 via vlan 1 with Ack 56/0

BEIGRP: Receive ACK packet from 192.168.20.204 via vlan 1 with Ack 0/56

BEIGRP: Send UPDATE packet to 192.168.20.141 via vlan 1 with Ack 56/88

BEIGRP: Send UPDATE packet to 192.168.20.204 via vlan 1 with Ack 56/143

BEIGRP: Receive UPDATE packet from 202.117.80.143 via vlan 2 with Ack 79/0

BEIGRP: Send HELLO packet to 202.117.80.143 via vlan 2 with Ack 0/79

BEIGRP: Receive ACK packet from 192.168.20.204 via vlan 1 with Ack 0/56

BEIGRP: Send QUERY packet to 224.0.0.10 via vlan 1 with Ack 60/0

BEIGRP: Send UPDATE packet to 224.0.0.10 via vlan 1 with Ack 61/0

FIeld	Description
Recv / Send / Enqueueing	Receives, sends or enqueueings packet to send -queue
HELLO / UPDATE / QUERY / ACK	Packet types that are received or sent
192.1.1.1	Neighbor IP address to send packet
vlan 2	In or out interface of packet
Ack 56/88	Acknowledgement number of packet/ sequence number of neighbor packet

related commands

debug ip beigrp fsm

60.6 debug ip beigrp transmit

Syntax

To display transmit event of BEIGRP packet, use the debug ip beigrp transmit command in EXEC mode

debug ip beigrp transmit [**ack | build | link | packetize | peerdown | startup**]

no debug ip beigrp transmit [**ack | build | link | packetize | peerdown | startup**]

Parameter

parameter	description
ack	(Optional) Traces events
build	(Optional)Traces BUILD events
link	(Optional)Traces LINK events
packetize	(Optional)Traces PACKETIZE events
peerdown	(Optional)Traces PEERDOWN events
startup	(Optional)Traces STARTUP events.

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command

related commands

debug ip beigrp fsm

60.7 default-metric

Syntax

To reset the default vector metric for the Enhanced Interior Gateway Routing Protocol (BEIGRP), use the **default-metric** command. To restore the default state, use the no form of this command

default-metric *bandwidth delay reliability loading mtu*

no default-metric

Parameter

parameter	description
bandwidth	Default bandwidth
delay	Default interface delay
reliability	Default interface reliability
loading	Default interface load
mtu	The default value for the maximum transmission unit (MTU)

default

bandwidth: 128kpbs

delay: 2000 (10ms)

reliability: 255 (255 indicates 100%)

loading: 255 (255 indicates 100%)

mtu: 1500

Command mode

router configuration

Usage guidelines

It is generally used with redistribute command to specify default metrics of route of other routing protocols assigned into BEIGRP. This command will trigger the new algorithm of related route that are previously assigned into BEIGRP

Forwarding static route, straight connected route and BEIGRP protocol route, you can not configure default-metric command, or you must configure this command

Example

The following example shows how the redistributed Routing Information Protocol (RIP) metrics are translated into EIGRP metrics with values as follows: bandwidth = 200, delay = 100, reliability = 100, loading = 200, and MTU = 1500:

default-metric 200 1000 100 200 1500

related commands

redistribute

60.8 Distance

Syntax

To allow the use of two administrative distances (internal and external) that could be a better route to a node,

use the distance beigrp command in routing switch configuration mode. To reset these values to their defaults, use the no form of this command

distance beigrp *internal-distance external-distance*

no distance beigrp

distance weight *ip-address ip-address-mask* [*ip-access-list*]

no distance weight *ip-address ip-address-mask* [*ip-access-list*]

Parameter

parameter	description
internal-distance	Administrative distance for Enhanced Internal Gateway Routing Protocol (BEIGRP) internal routes. The distance can be a value from 1 to 255
external-distance	Administrative distance for EIGRP external routes. The distance can be a value from 1 to 255
ip-address	BEIGRP neighbor IP address
ip-address-mask	BEIGRP neighbor IP address mask
ip-access-list	BEIGRP neighbor access list

default

internal-distance: 90

external-distance: 170

Command mode

router configuration

Usage guidelines

An administrative distance is to compare the priority of routes of different protocols. Therefore, adjustment on the administrative distance value of BEIGRP will affect the choice of routing switch to meet different demands od users

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list

Example

router beigrp 2

network 192.10.0.0 255.255.0.0

distance beigrp 100 200

distance 110 192.31.7.0 255.255.255.0

distance 220 128.88.1.0 255.255.255.0

In the above example, the routing switch beigrp global configuration command sets up BEIGRP internal administrative and external administrative to 100 and 200. The network routing switch configuration commands specify BEIGRP routing on networks 192.31.7.0/24 and 128.88.1.0/24 to 110 and 220

related commands

show ip protocol

60.9 Filter

Syntax

To allows us to filter the routes that learned or sent on the specified interface, use the filter command. Use the no form of this command to disable filter

filter {*interface*-type *interface*-number | *} {**in** | **out**} {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

no filter {*interface*-type *interface*-number | *} {**in** | **out**} {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

Parameter

parameter	description
interface-type interface-number	Interface type and number
*	all intefaces
in	Applies access-list to the incoming routing update
out	Applies access-list to the ourcoming routing update
access-list	Applies standard access list to filter routes, to define which network is sent and which network is suppressed in routing update
gateway	Filters gateway of route using standard access list
access-list-name	Standard IP access list number or name
prefix-list	Filters route using the prefix-list
prefix-list-name:	Standard IP prefix- list-name. This list defines which networks are received and which are surpressed.

default

none

Command mode

router configuration

Usage guidelines

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list

example

The following example permits only one network at 131.108.0.0 to be declared by BEIGRP routing process:

```
ip access-list standard 1
 permit 131.108.0.0 255.255.0.0
!
router beigrp 64
 filter * out access-list 1
 network 131.108.0.0
```

60.10 beigrp log-neighbor-changes

Syntax

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (BEIGRP) neighbor adjacencies, use the beigrp log-neighbor-changes command in router configuration mode. To disable the logging of changes in BEIGRP neighbor adjacencies, use the no form of this command

beigrp log-neighbor-changes

no beigrp log-neighbor-changes

Parameter

none

default

disabled

Command mode

router configuration

60.11 beigrp router-id

Syntax

To set the routing switch ID used by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the eigrp router-id command in router configuration mode. To remove the configured routing switch ID, use the no form of this command

beigrp router-id *ip-address*

no beigrp router-id

Parameter

parameter	description

ip-address	Router ID in dotted decimal notation

default

EIGRP automatically selects an IP address to use as the routing switch ID. Set the largest loopback interface as the routing switch ID if there is a loopback interface or set the largest direct-connect interface address as the the routing switch ID

Command mode

router configuration

60.12 ip beigrp bandwidth-percent

Syntax

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (BEIGRP) on an interface, use the ip bandwidth-percent eigrp command. To restore the default value, use the no form of this command

ip beigrp bandwidth-percent *percent*

no ip beigrp bandwidth-percent

Parameter

parameter	description
percent	Percent of bandwidth that EIGRP may use

default

50%

Command mode

interface configuration mode

Usage guidelines

For low speed lines, you can adjust the configuration of this command to restrict the enabled bandwidth for BEIGRP to avoid that BEIGRP affect the normal data transmission

Example

interface vlan 1

ip beigrp bandwidth-percent 100

The above example allows BEIGRP to use all bandwidth of the interface vlan 1

related commands

bandwidth

60.13 ip beigrp hello-interval

Syntax

To configure the hello interval for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the ip hello-interval eigrp command in interface configuration mode. To restore the default value, use the no form of this command

ip beigrp hello-interval *seconds*

no ip beigrp hello-interval

Parameter

parameter	description
second	Hello interval (in seconds)

default

5 seconds

Command mode

interface configuration mode

Usage guidelines

example

interface vlan 1

ip beigrp hello-interval 20

The above example sets 20 seconds as the hello interval for vlan 1:

related commands

ip beigrp hold-time

60.14 ip beigrp hold-time

Syntax

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the ip hold-time eigrp command in interface configuration mode. To restore the default value, use the no form of this command

ip beigrp hold-time *seconds*

no ip beigrp hold-time

Parameter

parameter	description
second	Hold time is in seconds if do not receive any BEIGRP

default

15 seconds

Command mode

interface configuration mode

Usage guidelines

example

Interface vlan 1

ip beigrp hold-time 60

The above example sets 60 seconds the hold time for vlan 1:

related commands

ip beigrp hello-interval

60.15 ip beigrp passive

Syntax

To enable interacting BEIGRP routing update on a certain interface, use the ip beigrp passive command. Use the no form of this command to restore the default value

ip beigrp passive

no ip beigrp passive

parameter

none

default

The interface is not in passive mode

Command mode

interface configuration mode

Usage guidelines

If the ip beigrp passive is configured on an interface, then no routing update is received on this interface, and also no neighborhood relation is established between this interface and any accessible neighbors. But a direct route genereate on this interface will be broadcast by other interface that runs the BEIGRP

example

The following command set vlan 1 as the passive interface:

interface vlan 1

ip beigrp passive

60.16 ip beigrp split-horizon

Syntax

To enable Enhanced Interior Gateway Routing Protocol (BEIGRP) split horizon, use the ip beigrp split-horizon command in interface configuration mode. To disable split horizon, use the no form of this command

ip beigrp split-horizon

no ip beigrp split-horizon

Parameter

none

default

The behavior of this command is enabled by default

Command mode

interface configuration mode

Usage guidelines

Using this command is to prevent route cycle, so you must confirm that it will not cause any bad effects before turn off the split horizon

example

interface vlan 1

no ip beigrp split-horizon

The above example disables split horizon on vlan 1:

60.17 metric weights

Syntax

To tune Enhanced Interior Gateway Routing Protocol (BEIGRP) metric calculations, use the metric weights command. To reset the values to their defaults, use the no form of this command

metric weight k1 k2 k3 k4 k5

no metric weight

Parameter

parameter	description
k1,k2,k3,k4,k4	Constants that convert an EIGRP metric vector into a scalar quantity

default

k1: 1

k2: 0

k3: 1

k4: 0

k5: 0

Command mode

router configuration

Usage guidelines

The tuning of the EIGRP metric calculation for a composite metric adopts two steps:

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

Composite metric = K1*BW*256 + K2 * BW/(256 - load) + K3 * DLY * 256,

BW10Gbps/ bandwidth

DLYDelay time, 10 milliseconds

If k5 does not equal zero, an additional operation is performed:

Composite metric = Composite metric * K5/(reliability + K4)

K2, K4 and K5 are the left objects of IGRP, compatible with Eigrp protocol of Cisco. In general, Load and Reliability are not used in composite metric algorithm. Therefore, do not change the default value of K2, K4 and K5, unless you confirm that will not cause bad effect, to prevent unexpected result on route decision

example

router beigrp 2

network 131.108.0.0 255.255.0.0

metric weights 2 0 2 0 0

related commands

bandwidth

delay

60.18 Network

Syntax

To specify the network for an Enhanced Interior Gateway Routing Protocol (BEIGRP) routing process, use the network command in routing switch configuration mode. To remove an entry, use the no form of this command

network *network-number* [*netmask*]

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

Parameter

parameter	description
network-number	Network address
netmask	Network mask

default

none

Command mode

router configuration

Usage guidelines

Various network statements (network commands) can be configured on a routing switch, to enable BEIGRP dynamic routing protocol to run on many networks; use the default mask if there is no configured mask

example

router beigrp 2

network 131.108.0.0 255.255.0.0

network 122.11.2.0

related commands

router beigrp

60.19 Offset

Syntax

To add an offset to incoming and outgoing metrics to routes learned via Enhanced Interior Gateway Routing Protocol (BEIGRP), use the offset command in router configuration mode. To remove an offset list, use the no form of this command

offset {*type number* | *****} {**in** | **out**} *access-list-name offset*

no offset {*type number* | *****} {**in** | **out**}

Parameter

parameter	description

In	Applies the access list to incoming metrics
Out	Applies the access list to outgoing metrics
access-list-name	Standard access list name to be applied
Offset	Positive offset to be applied to metrics for networks matching the access list
Type	(Optional) Interface type to which the offset list is applied
Number	(Optional) Interface number to which the offset list is applied

default

none

Command mode

router configuration

Usage guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric

BEIGRP is a vector metric, so the offset is added to delay

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list

example

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 21:

offset * out 21 10

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

offset e0/0 in 21 10

related commands

ip access-list

60.20 redistribute

Syntax

To redistribute routes from other routing protocols into the local BEIGRP routing process routing table, use the redistribute command

redistribute protocol *process* **route-map** *name*

redistribute protocol *process* **[route-map]**

Parameter

parameter	description
protocol	Source protocol from which routes are being redistributed. It must be one of following keywords: bgp, ospf, static , connected, and rip
process	(Optional) For bgp or bigp, this parameter indicates the 16-digit autonomous number. For OSPF, this parameter indicates the relevant OSPF process ID of the routes need to be redistributed. This marks the rouing process. It is a non-zero decimal number. For rip, there is no need to mark the process
route-map	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to IS-IS. If not specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported
name	Name character string of route-map

default

none

Command mode

BEIGRProuter configuration

Usage guidelines

To redistribute direct routes, static routes and routes from other BEIGRP process, the default-metric command is not necessarily to be configured;otherwise, the default-metric must be configueid

example

default-metric 64 250 255 255 1500

redistribute ospf 1

60.21 router beigrp

Syntax

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the router beigrp command in global configuration mode. To delete the BEIGRP routing process, use the no form of this command

router beigrp *autonomous-system-number [*vrf *vrf-name]*

no router beigrp *autonomous-system-number [*vrf *vrf-name]*

Parameter

parameter	description

autonomous-system-number	Autonomous system number that identifies the routes to the other BEIGRP routers
vrf-name	Specifies the VRF to which the BEIGRP process belongs

default

none

Command mode

global configuration mode

Usage guidelines

This command can be used to operate multiple BEIGRP processes

example

The following example configures EIGRP process 30:

router beigrp 30

related commands

network

60.22 show ip beigrp interface

Syntax

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the show ip beigrp interfaces command

show ip beigrp interfaces [**interface-type** *interface-number* | *as-number*]

Parameter

parameter	description
as-number	Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process
interface	Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface

default

none

Command mode

All configuration modes except user mode

Usage guidelines

Use the show ip eigrp interfaces command to learn information about BEIGRP dynamic routing relating to those interfaces

related commands

None

60.23 show ip beigrp neighbors

Syntax

To display neighbors discovered by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the show ip eigrp neighbors command in EXEC mode

show ip beigrp neighbors [*interface-type interface-number* | *as-number*] [*detail*]

Parameter

parameter	description
as-number	Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process
interface	Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface
detail	Displays detailed neighbor information

default

none

Command mode

All configuration modes except user mode

Usage guidelines

Use the show ip beigrp neighbors command to determine what neighbours they are and when neighbors become active and inactive. It is also useful for debugging certain types of transport problems

example

Router# show ip beigrp neighbors

Information of BEIGRP neighbors with AS 1024

Address interface hold uptime Q_cnt Seq

192.168.20.204 vlan 1 15 00:08:06 0 159

202.117.80.143 vlan 2 10 00:08:05 0 100

192.168.20.141 vlan 1 12 00:07:38 0 254

field	explanation
AS 64	Autonomous system number
Address	IP address of the BEIGRP peer
Interface	Interface on which the router is receiving hello packets from the peer
Hold	Length of time that the software will wait to hear from the peer before declaring it down
Uptime	Elapsed time since the local router first heard from this neighbor
Q Count	Number of EIGRP packets that the software is waiting to send
Seq	Sequence number of the last update that was received from this neighbor

related commands

None

60.24 show ip beigrp protocol

Syntax

To display the Enhanced Interior Gateway Routing Protocol (BEIGRP) routing protocol process parameter and statistics, use the show ip beigrp protocols command

show ip beigrp protocols [*as-number*]

Parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified, it will display only the parameters and statistics of this BEIGRP process

Command mode

All configuration modes except user mode

Usage guidelines

This command can be used to check BEIGRP topology table at any time

example

R142#show ip bei pro

Protocol Information of BEIGRP with AS 1024:

Metric Weight: K1=1, K2=0, K3=1, K4=0, K5=0.

Filter * in access-list in12

Filter * out access-list ou12

Offset * in in23 12

Offset * out ou23 12

Redistributing: connect, ospf 1, ospf 2

Automatic network summarization is enable.

Active-time: 3(minutes)

Routing for Networks:

192.168.20.0/24

10.0.0.0/8

167.20.0.0/16

202.117.80.0/24

Distance: internal 90, external 170

Active Route:

related commands

None

60.25 show ip beigrp topology

Syntax

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the show ip beigrp topology command in privileged EXEC mode

show ip beigrp topology [[as-number active | all-links | pending | summary | zero-successors] | [network-number subnet-mask]]

Parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified, it will display only the topology table of BEIGRP process
network-number	Displays detailed information about the specified network
subnet-mask	(Optional) Subnet mask
active	(Optional) Displays only active entries in the BEIGRP topology table
all-link	(Optional) Displays all entries in the BEIGRP topology table

pending	(Optional) Displays all entries in the BEIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor
summary	(Optional) Displays a summary of the BEIGRP topology table
zero-successors	(Optional) Displays available routes in the EIGRP topology table

default

none

Command mode

All configuration modes except user mode

Usage guidelines

This command can be used to check BEIGRP topology table at any time

example

```
Router# show ip beigrp topology
P 10.10.10.0/24 successors: 1 FD: 13056
  via connect(Loopback1) Metric: 13056/0
P 167.20.0.0/16 successors: 1 FD: 261132
  via 202.117.80.143(vlan 1) Metric: 261132/258560
P 192.166.100.0/24 successors: 1 FD: 281856
  via redistribute Metric: 281856/0
P 192.168.20.0/24 successors: 1 FD: 258560
  via connect(vlan 2) Metric: 258560/0
P 202.1.1.0/24 successors: 1 FD: 297246988
  via 192.168.20.204(vlan 2) Metric: 297246988/297244416
P 202.117.80.0/24 successors: 1 FD: 258560
  via connect(vlan 1) Metric: 258560/0
A 202.117.93.0/24 successors: 1 FD: unaccessible, R serno: 32
  via 192.168.20.141(vlan 2) Metric: 271372/13056
SIA-Info: (active: 00:02:20 query-origin: Local origin)
  Unreplied Neighbors:
  via 202.117.80.143, vlan 1
P 202.192.168.0/24 successors: 1 FD: 284172
```

via 192.168.20.204(vlan 2) Metric: 284172/281600

field	description
160.89.90.0 and so on	Destination network number
255.255.255.0	Destination network mask
successors	Number of successors
FD	Feasible distance
Via	Gateway address
vlan 2	Interface from which this information was learned
SIA-Info	active routing information
active	Lasting time when entering Active status
query-origin	Origin of entering query state
Unreplied Neighbors	Neighbor lists that are not received reply

related commands

None

60.26 show ip beigrp traffic

Syntax

To display the flow information of Enhanced Interior Gateway Routing Protocol (BEIGRP) packets sent and received, use the show ip beigrp traffic command in EXEC mode

show ip beigrp traffic [*as-number*]

Parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified ,then display the flow statistics information

default

none

Command mode

All configuration modes except user mode

Usage guidelines

Use this command to check the flow statistics information of BEIGRP packets sent and received at any time

example

R142#show ip bei tra

Traffic Statistics of BEIGRP 1024

Packet Type Hello Update Query Reply ACK

Send/Receive 770/1021 133/44 29/7 7/9 60/147

related commands

None

Chapter 61 OSPF Configuration Commands

61.1 area authentication

Syntax

To enable authentication for an Open Shortest Path Firstly (OSPF) area, use the area authentication command in routing switch configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command

area *area-id* **authentication** {**simple | message-digest**}

no area *area-id* **authentication**

no area *area-id*

Parameter

parameter	description
area-id	Identifier of the area for which authentication is to be enabled
simple	(Optional)authentication information, Plain text authentication
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument

Default value

no authentication of interface receiving OSPF packet by default

Command mode

router configuration

Usage guidelines

The authentication value will be added into OSPF packet.The authentication type of all routing swithces in the same area must be the same.The authentication password for all OSPF routing switches on a network must be the same if they are to communicate with each other via OSPF

Example

The following example mandates authentication simple for areas 0 and 36.0.0.0.

interface VLAN1

ip address 131.119.251.201 255.255.255.0

ip ospf password 0 adcdefgh

!

interface VLAN2

```
 ip address 36.56.0.201 255.255.0.0
ip ospf password 0 ijklmnop
!
router ospf 1
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 network 131.119.0.0 255.255.0.0 area 0
 area 0 authentication simple
 area 36.0.0.0 authentication simple
!
```

Related commands

ip ospf password

ip ospf message-digest-key

61.2 area default-cost

Syntax

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the area default-cost command in router address family topology or routing switch configuration mode. To remove the assigned default route cost, use the no form of this command

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

no area *area-id*

Parameter

parameter	description
area-id	Identifier for the stub area
cost	Cost for the default summary route used for a stub

Default value

cost.1

Command mode

OSPF Routing configuration mode

Usage guidelines

This command is used only on an routing switch attached to a stub area or NSSA

After configured the area stub default-information-originate command, the routing switch will send LSA(SUM-NER-LSA) including default router information to correspondent field, the cost configured I this command is the correspondent cost used in LSA

Note:

To remove the specified area from the software configuration, use the no area area-id command (without other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link

Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 area 36.0.0.0 default-cost 20
 area 36.0.0.0 stub
!
```

Related commands

area nssa

area stub

61.3 area filter

Syntax

To filter Type-3 LSA of in/out this area, run the following command. To return to the default setting, use the no form of this command

area *area-id* **filter** {**in** |**out**} {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}

no area *area-id* **filter** {**in** | **out**}

no area *area-id*

Parameter

Parameter	Description
area-id	Domain which filters Type-3 LSA. It can be a decimal numeral or an ip address

in	In ABR, filter Type-3 LSA sent to this area
out	In ABR, filter Type-3 LSA sent from this area to other areas
access-list-name	Name of access list
prefix-list-name	Name of prefix list

Default value

Disabled

Command mode

OSPF Routing configuration mode

Usage guidelines

The command only works on the ABR, but is not available to the area inner route. In direction in, Type-3 LSA of ABR sent to this area does not include the filtered network segment. This rule is also applicable to area-range segment of other areas; in direction out, Type-3 LSA of ABR sent to this area does not include the filtered network segment. If all sub-segments covered by an area-range are filtered, the area-range will not generate Type-3 LSA

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval,area nssa-range, area range, area stub, and area virtual-link

Example

The following example shows how to configure area 36.0.0.0 which neither receives Type-3 LSA including in 192.0.0.0/8, nor generates Type-3 LSA including in 36.0.0.0/8.

```
!
interface VLAN1
 ip address 192.42.110.201 255.255.255.0
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 network 192.0.0.0 255.0.0.0 area 0
 area 36.0.0.0 filter in prefix-list bd1
```

area 36.0.0.0 filter out prefix-list bd2

!

!

ip prefix-list bd1 seq 5 deny 192.0.0.0/8

ip prefix-list bd2 seq 5 deny 36.0.0.0/8

!

Related command

area authentication

61.4 area nssa

Syntax

To configure a NSSA area, run the following command. To return to the default setting, use the no form of this command

area *area-id* **nssa** [**default-information-originate** [**metric** *value* | **metric-type** {*1* | *2*}] |**no-redistribute** | **no-summary** | **translate-always**]

no area *area-id* **nssa** [**default-information-originate** | **no-redistribute** | **no-summary** | **translate-always**]

no area *area-id*

Parameter

Parameter	Description
area-id	Area-ID of NSSA. It can be a decimal numeral or an ip address.
default-information-originate	(Optional) For ABR, if this command is configured but without configuring command **no-summany**, whether there is a default route, one Type-7 LSA will be generated to send the default route to the area; if command **no-summany** is configured, a Type-3 LSA will be generated to send the default route to the area. For ASBR, after configuration, only when the main routing table has a default route can Type-7 LSA be generated to sent a default route to the area
metric	(Optional) default metric
metric-type	(Optional) default metric type of the route
no-redistribute	(Optional) The command is used to diable introduce AS outer route to NSSA by the form of Type-7 LSA. Usually it is only used in ABR of NSSA and ASBR or OSPF.
no-summary	(Optional) The command is only used in ABR of NSSA and disable ABR router forwarding Type-3 LSA to NSSA. After configuration, NSSA ABR send one default route to the area by generating one Type-3 LSA and does not send other Type-3 LSA to the area (The area is also called NSSA Totally Stub)
translate-always	(Optional) Only used for ABR of NSSA domain. ABR works for translating Type-7 LSA into

Type-5 LSA

Default value

Non-NSSA area

Command mode

OSPF Routing configuration mode

Usage guidelines

The command "area nssa" must be configured on all routers and acess servers in NSSA area

For further decreasing the amount of LSA, use command **no-summary** to sending summarizing LSA to NSSA on ABR

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval,area nssa-range, area range, area stub, and area virtual-link

Example

The following example shows how to configure 36.0.0.0 as NSSA area

```
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 area 36.0.0.0 nssa
 redistribute static
!
```

Related command

area authentication

area default-cost

redistribute

61.5 area nssa-range

Syntax

To translate Type-7 LSA for route aggregation, run the following command. To return to the default setting, use the no form of this command

area *area-id* **nssa-range** *address mask* [**advertise | not-advertise | tag** *value*] [**cost** *cost*] [**cost** cost_value]

no area *area-id* **nssa-range** *address mask*

no area *area-id*

Parameter

Parameter	Description
area-id	Domain of Type-7 LSA route aggregation. It can be a decimal numeral or an ip address
address	Destination IP address of the aggregation route
mask	The network mask of aggregation route.
advertise	(Optional) Advertise after aggregation
not-advertise	(Optional) Not-advertise after aggregation
tag	(Optional) Tag of aggregation route
value	Route tag. The value ranges from 0 to 4294967295. The default value is 0
cost	(Optional) Cost of aggregation route
cost_value	Cost value of aggregation route. The value ranges from 0 to 16777215. The default value is the max cost of all aggregated route

Default value

Disabled

Command mode

OSPF Routing configuration mode

Usage guidelines

The command can only be configured on the non-trunk domain

If the local router is ABR and the translation router of NSSA, the command “area nssa-rang” will aggregates Type-7 LSA and generates Type-5 LSA; for translation router not in the NSSA, there is no aggregation

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval,area nssa-range, area range, area stub, and area virtual-link

Example

The following example shows how to configure route aggregation of translatable Type-7 LSA in segment 50.0.0.0 of ABR

!

interface VLAN1

```
 ip address 192.42.110.201 255.255.255.0
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 network 192.0.0.0 255.0.0.0 area 0
 area 36.0.0.0 nssa
 area 36.0.0.0 nssa-range 50.0.0.0 255.0.0.0
!
```

Related command

area nssa

61.6 area nssa-translate-interval

Syntax

To configure a time interval a translater elected by Type-7 LSA works after being replaced by another one. To return to the default setting, use the no form of this command

area *area-id* **nssa-translate-interval** *interval*

no area *area-id* **nssa-translate-interval**

no area *area-id*

Parameter

Parameter	Description
area-id	Area-ID of NSSA. It can be a decimal numeral or an ip address
interval	Time interval. Unit: s

Default value

40s

Command mode

OSPF Routing configuration mode

Usage guidelines

The command can only be configured on the non-trunk area

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval, area nssa-range, area range, area stub, and area virtual-link

Example

The following example shows how to configure the time interval of area 36.0.0.0 to 100s.

```
!
interface VLAN1
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 area 36.0.0.0 nssa
 area 36.0.0.0 nssa-translate-interval 100
 redistribute static
!
```

Related command

area nssa

61.7 area range

Syntax

To consolidate and summarize routes at an area boundary, use the **area range** command. To disable this function, use the no form of this command

area *area-id* **range** *address mask* **[advertise | not-advertise**] [**cost** *value*]

no area *area-id* **range** *address mask*

no area *area-id*

Parameter

parameter	description

area-id	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix
address	IP address
mask	IP address mask
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA)
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks

Default value

This command is disabled by default

Command mode

OSPF Routing configuration mode

Usage guidelines

The area range command is used only with Area Border Routing switches. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR

Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization

Multiple area range routing switch configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area default-cost, area nssa, area range, area stub, and area virtual-link

Example

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
!
interface VLAN1
 ip address 192.42.110.201 255.255.255.0
 no ip directed-broadcast
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
 no ip directed-broadcast
!
```

```
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 network 192.0.0.0 255.0.0.0 area 0
 area 0 range 192.42.110.0 255.255.255.0
 area 36.0.0.0 range 36.0.0.0 255.0.0.0
!
```

61.8 area stub

Syntax

To define an area as a stub area, use the area stub command. To disable this function, use the no form of this command

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

no area *area-id* **stub**

no area *area-id*

Parameter

parameter	description
area-id	Identifier for the stub area; either a decimal value or an IP address
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area

Default value

No stub area is defined

Command mode

OSPF Routing configuration mode

Usage guidelines

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal route sent into a stub area by an ABR switch

There are two stub area router configuration commands: the stub and default-cost options of the area routing switch configuration command. In all routing switches attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR switch to prevent it from sending summary LSAs (LSA type 3) into the stub

area

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link

Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 area 36.0.0.0 default-cost 20
 area 36.0.0.0 stub
!
```

Related commands

area authentication

area default-cost

61.9 area virtual-link

Syntax

To define a virtual link, use the area virtual-link command

area *area-id* **virtual-link** *neighbor-ID* [**authentication** simple | message-digest] [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*][**password** [*0* | *7*] *pass-string*] [**message-digest-key** key-id MD5 [0 | 7] md5-string]

no area area-id **virtual-link** neighbor-ID [authentication] [dead-interval [hello-interval] [retransmit-interval][transmit-delay][password] [message-digest-key key-id]

Parameter

parameter	description
area-id	Area ID assigned to the transit area for the virtual link
neighbor-id	Router ID associated with the virtual link neighbor
simple	Plain text authentication. The value must be the same for all routing switches and access

	servers attached to a common network
message-digest	Enables Message Digest 5 (MD5) on virtual-link. The value must be the same for all routing switches and access servers attached to a common network
dead-value	Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The value must be the same for all routing switches and access servers attached to a common network
hello-value	Time (in seconds) between the hello packets that the software sends on an interface. The value must be the same for all routing switches and access servers attached to a common network
retrans-value	Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be the same for all routing switches and access servers attached to a common network
dly-value	Delay value in seconds to inform LSA on virtual-link for a routing switch. The configured value on both sides of the virtual-link should be the same
pass-string	If virtual-link uses plain text authentication, the the maximum character of the configured password should be 8. The configuied value on both sides of the virtual-link should be the same
key-id	If virtual-link uses MD5 authentication, the valid range of the used MD5 key should from 1 to 255. The configured value on both sides of the virtual-link should be the same
MD5-String	Configures MD5 password, which is 16-character at most. The configured value on both sides of the virtual-link should be the same
0|7	Designate the key type: plaintext (0) or ciphertext (7)

Default value

No virtual-link is configured

Default value of other parameters are as follows:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s, no authentication

Command mode

OSPFrouter configuration

Usage guidelines

To establish a virtual link, user should configure both sides of the virtual link. The virtual link will fail if this command is only configured on one side

The parameter-id must be a non-zero character, for the virtual link and the transit areda must be a non-backbone area. The configured area-id of the virtual link must be the same

The neighbor-ID must be the same as the ospf router-id on the remote side during configuration, or the virtual link will not be established. Even if the configured neighbor-ID is another IP address of the other side

You must make sure that all parameters on both sides must be the same

The authentication parameters that configured on virtual-link become effective only when configured authentication types of virtual-link or configured the relevant authentication methods in backbone are (via the command area authentication)Only one kind of authentication parameter can be configured on virtual-link, that is, the MD5 and the plain text authenticationm are mutually exclusive

Use the command no area area-id veitual-link neighbor-ID to cancel the formerly-configured virtual link

Use the command show ip ospf virtual-link to check state of the virtual link

Note:

no area area-id **(no other parameters)**

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval, area nssa-range, area range, area stub, and area virtual-link

Example

The following example configured a virtual link between router A and router B:

The configuration on router A (router-id: 200.200.200.1):

```
!
router ospf 100
  network 192.168.20.0 255.255.255.0 area 1
  area 1 virtual-link 200.200.200.2
!
```

The configuration on router B(router-id: 200.200.200.2):

```
!
router ospf 100
  network 192.168.30.0 255.255.255.0 area 1
  area 1 virtual-link 200.200.200.1
!
```

Related commands

show ip ospf virtual-link

61.10 auto-cost

Syntax

To configure reference-bandwidth value, run the following command. To return to the default setting, use the no form of this command

auto-cost reference-bandwidth *value*

no auto-cost reference-bandwidth

Parameter

Parameter	Description
value	Reference-bandwidth value for calculating link cost. The value ranges from 1 to 4294967. Unit:

Mbps

Default value

100Mbp

Command mode

OSPF Routing configuration mode

Usage guidelines

If the command is not configured, OSPF calculates cost according to the link bandwidth(cost is equal to bandwidth reference value divided by bandwidth; if the cost is larger than 65535. The max cost is 65535)

If the command is configured, OSPF does not calculate cost based on the link bandwidth, but based on the configured link

Example

The following example shows how to configure the bandwidth reference of the link to 1000Mbps:

!

interface VLAN2

ip address 36.56.0.201 255.255.0.0

!

router ospf 201

auto-cost reference-bandwidth 1000

network 36.0.0.0 255.0.0.0 area 36.0.0.0

!

Related command

ip ospf cost

61.11 bfd all-interfaces

Syntax

To enable bfd linkage function on all ospf interfaces, use the **bfd all-interfaces** command. To restore the default value, use the **no bfd all-interfaces** command

bfd all-interfaces

no bfd all-interfaces

Parameter

None

Default

No bfd linkage

Command mode

OSPF Routing configuration mode

Usage guidelines

Configuring bfd all-interfaces will enable the bfd linkage function of all ospf interfaces, except for interfaces configured with the **ip ospf bfd disable** command. Command **bfd all-interfaces** is usually configured when there are many ospf interfaces

Example

The following example shows how to configure the bfd function of the ospf interface(except for vlan2)

```
interface VLAN1
 ip address 36.56.0.201 255.255.0.0
!
interface VLAN2
 ip address 36.57.0.201 255.255.0.0
 ip ospf bfd disable
!
interface VLAN3
 ip address 36.58.0.201 255.255.0.0
!
router ospf 201
 router-id 1.2.2.1
        network 36.0.0.0 255.0.0.0 area 36.0.0.0
        bfd all-interfaces
!
```

Related command

ip ospf bfd

61.12 debug ip ospf adj

Syntax

To monitor Open Shortest Path Firstly (OSPF)-related estabilishment process , use the debug ospf adj command

debug ip ospf adj

Parameter

none

Default

none

Command mode

EXEC

Usage guidelines

User can check the process of OSPF-related estabilishment process from the output of this command

Example

Switch # debug ip ospf adj

OSPF[1]: Interface 0.0.0.0 on VLAN1 going Up

OSPF[1]: 2 Way Communication to 192.85.1.5 on VLAN1, state 2WAY

OSPF[1]: 2 Way Communication to 1.1.1.1 on VLAN1, state 2WAY

OSPF[1]: Interface 0.0.0.0 on VLAN1 Waittmr expired

OSPF[1]: NBR 1.1.1.1 on VLAN1 Adjacency OK, state EXSTART.

OSPF[1]: NBR 192.85.1.5 on VLAN1 Adjacency OK, state EXSTART.

OSPF[1]: NBR 192.85.1.5 Negotiation Done. We are the SLAVE. seq 0x25c83

OSPF[1]: NBR 192.85.1.5 on VLAN1 Negotiation Done. We are the SLAVE

OSPF[1]: Exchange Done with 192.85.1.5 on VLAN1

OSPF[1]: Loading Done with 192.85.1.5 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 192.85.1.5 on VLAN1, database Synchronized (FULL)

OSPF[1]: NBR 192.85.1.4 Negotiation Done. We are the MASTER. seq 0x12b

OSPF[1]: NBR 1.1.1.1 on VLAN1 Negotiation Done. We are the MASTER

OSPF[1]: Exchange Done with 1.1.1.1 on VLAN1

OSPF[1]: Loading Done with 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)

……

61.13 debug ip ospf events

Syntax

To monitor OSPF interface and OSPF-related events, , use the debug ip ospf events command

debug ip ospf events

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF interface and OSPF-related adjacency events from the ouput of this command

Example

Switch # debug ip ospf events

OSPF: Receive [MSG_OSPF_PROTO_UP] message, index=26

OSPF[1]: Interface VLAN1 going Up

OSPF: INTF(192.85.1.0) event INTF_UP

OSPF[1]: Interface 192.85.1.0 on VLAN1 going Up

OSPF: Receive [MSG_OSPF_TASKPOLICY_CHANGE] message

OSPF: NBR(192.85.1.5) event HELLO_RX

OSPF: NBR(192.85.1.4) event HELLO_RX

OSPF: NBR(192.85.1.4) event TWOWAY

OSPF[1]: 2 Way Communication to 1.1.1.1 on VLAN1, state 2WAY

OSPF: NBR(192.85.1.5) event TWOWAY

OSPF[1]: 2 Way Communication to 192.85.1.5 on VLAN1, state 2WAY

OSPF: INTF(192.85.1.0) event WAIT_TIMER

OSPF[1]: Interface 192.85.1.0 on VLAN1 Waittmr expired

OSPF: NBR(192.85.1.4) event ADJ_OK

OSPF[1]: NBR 1.1.1.1 on VLAN1 Adjacency OK, state EXSTART.

OSPF: NBR(192.85.1.5) event ADJ_OK

OSPF[1]: NBR 192.85.1.5 on VLAN1 Adjacency OK, state EXSTART.

OSPF[1]: NBR 192.85.1.4 Negotiation Done. We are the MASTER. seq 0x3a1

OSPF: NBR(192.85.1.4) event NEGO_DONE

OSPF[1]: NBR 1.1.1.1 on VLAN1 Negotiation Done. We are the MASTER

OSPF: NBR(192.85.1.4) event EXCH_DONE

OSPF[1]: Exchange Done with 1.1.1.1 on VLAN1

OSPF: NBR(192.85.1.4) event LOAD_DONE

OSPF[1]: Loading Done with 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: NBR 192.85.1.5 Negotiation Done. We are the SLAVE. seq 0x25efb

OSPF: NBR(192.85.1.5) event NEGO_DONE

OSPF[1]: NBR 192.85.1.5 on VLAN1 Negotiation Done. We are the SLAVE

OSPF: NBR(192.85.1.5) event EXCH_DONE

OSPF[1]: Exchange Done with 192.85.1.5 on VLAN1

OSPF: NBR(192.85.1.5) event LOAD_DONE

OSPF[1]: Loading Done with 192.85.1.5 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 192.85.1.5 on VLAN1, database Synchronized (FULL)

……

61.14 debug ip ospf flood

Syntax

To display OSPF-related database pervasion process, use the debug ip ospf flood command

debug ip ospf flood

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF-related database pervasion process from the output of this command

Example

Switch # debug ip ospf flood

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 15 SEQ 0x80000004 in area 0

OSPF[1]: not_my_lsa new DB(192.85.1.5) type 1 AGE 15 SEQ 0x80000004 CHKS 0x2d94

OSPF[1]: recv UPDATE, type 1 LSID 1.1.1.1 ADV_RTR 1.1.1.1 AGE 15 SEQ 0x80000003 in area 0

OSPF[1]: not_my_lsa new DB(1.1.1.1) type 1 AGE 15 SEQ 0x80000003 CHKS 0x7281

OSPF[1]: recv UPDATE, type 2 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 20 SEQ 0x80000001 in area 0

OSPF[1]: not_my_lsa new DB(192.85.1.5) type 2 AGE 20 SEQ 0x80000001 CHKS 0x7d66

OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 192.85.1.5 on VLAN1, database Synchronized (FULL)

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 8 SEQ 0x80000002 in area 0

OSPF[1]: when add DB(192.85.1.1) type 1, we fount it

OSPF[1]: recv self originate DB(192.85.1.1) type 1, same instance

OSPF[1]: recv UPDATE, type 2 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 1 SEQ 0x80000002 in area 0

OSPF[1]: when add DB(192.85.1.5) type 2, we fount it

OSPF[1]: not_my_lsa MORE_RECENT DB(192.85.1.5) type 2 AGE 20 SEQ 0x80000001 CHKS 0x7d66

OSPF[1]: Send UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 1 SEQ 0x80000003 in the area 0

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 2 SEQ 0x80000003 in area 0

OSPF[1]: when add DB(192.85.1.1) type 1, we fount it

OSPF[1]: recv self originate DB(192.85.1.1) type 1, same instance

OSPF[1]: recv UPDATE, type 2 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 1 SEQ 0x80000003 in area 0

OSPF[1]: when add DB(192.85.1.5) type 2, we fount it

OSPF[1]: not_my_lsa MORE_RECENT DB(192.85.1.5) type 2 AGE 1 SEQ 0x80000002 CHKS 0xf6cf

……

61.15 debug ip ospf lsa-generation

Syntax

To display OSPF-related LSA generation process, use the debug ip ospf lsa generation command

debug ip ospf lsa-generation

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF interface and adjacency events from the output of this command

Example

router# debug ip ospf lsa-generation

……

OSPF[1]: addLSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: add new LSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: Build RTR_LSA for area 0, rID 192.85.1.1, seq0x80000001

OSPF[1]: addLSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: find the same LSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: Build RTR_LSA for area 0, rID 192.85.1.1, seq0x80000002

OSPF[1]: addLSA, type:1, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0

OSPF[1]: add new LSA, type:1, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0

OSPF[1]: addLSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0

OSPF[1]: add new LSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0

OSPF[1]: addLSA, type:2, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0

OSPF[1]: add new LSA, type:2, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0

OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: addLSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0

OSPF[1]: find the same LSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0

……

61.16 debug ip ospf packet

Syntax

To display OSPF packets, use the debug ip ospf packet command

debug ip ospf packet [ack | dd | hello | update | request]

Parameter

Parameter	Description
ack	Monitors OSPF ACK packets
dd	Monitors OSPF DD packets
hello	Monitors OSPF Hello packets
update	Monitors OSPF Update packets
request	Monitors OSPF Request packets

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF interface and adjacency events from the output of this command

Example

Switch# debug ip ospf packet

OSPF: Recv a packet from source: 192.85.1.4 dest 224.0.0.5

OSPF[1]: Recv HELLO from 1.1.1.1(addr: 192.85.1.4) area 0 from VLAN1

OSPF[1]: End of hello processing

OSPF: Recv IP_SOCKET_RECV_PACKET message, length=72

OSPF: Recv a packet from source: 192.85.1.5 dest 224.0.0.5

OSPF[1]: Recv HELLO from 192.85.1.5(addr: 192.85.1.5) area 0 from VLAN1

OSPF[1]: End of hello processing

OSPF[1]: Send HELLO to 224.0.0.5 on VLAN1. HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 52

OSPF: Recv IP_SOCKET_RECV_PACKET message, length=72

OSPF: Recv a packet from source: 192.85.1.4 dest 224.0.0.5

OSPF[1]: Recv HELLO from 1.1.1.1(addr: 192.85.1.4) area 0 from VLAN1

OSPF[1]: End of hello processing

……

OSPF: Recv a packet from source: 192.85.1.5 dest 224.0.0.5

OSPF[1]: recv UPDATE packet from 192.85.1.5 (addr: 192.85.1.5) area 0 from VLAN1 len 64 advcnt 1

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 7 SEQ 0x80000002 in area 0

OSPF[1]: Send ACK, type 1, LSID 192.85.1.1, ADV_RTR 192.85.1.1, AGE 5, SEQ 0x80000002

OSPF[1]: Send ACK to 192.85.1.5(RID 192.85.1.5) len 44 on VLAN1

……

61.17 debug ip ospf restart

Syntax

To moniter the smooth restart process of OSPF, run the following command

debug ip ospf restart

Parameter

None

Default value

None

Command mode

Exec

Usage guidelines

The command is used to output information and show the smooth restart process of OSPF

Example

GR Restarter end:

Switch# debug ip ospf restart

OSPF: Recv MSG_OSPF_GRACEFUL_RESTART message

OSPF: Build grace-LSA, adv_rtr:5.5.5.5, in area 0, at interface VLink 0.0.0.0

OSPF: Build grace-LSA, adv_rtr:5.5.5.5, in area 1, at interface VLAN1

OSPF: grace-LSAs have been flooded out. switch redundant

OSPF: The OSPF process 1 is restarting gracefully now.

OSPF: Recv MSG_OSPF_RESTART message

OSPF: OSPF process 1 is restarting

OSPF: Database resynchronized with 12.12.12.12 on VLAN1 done, to FULL

OSPF: OSPF process 1 has reestablished all its adjacencies. GR successfully

OSPF: Recv MSG_OSPF_GR_TERMINATE message

OSPF: GR of OSPF process 1 terminated

GR Helper end:

router# debug ip ospf restart

OSPF: IETF GR Received grace-LSA from 5.5.5.5(addr: 192.167.1.1) on VLink 192.167.1.1

OSPF: IETF GR Validate grace-LSA from nbr 5.5.5.5 on VLink 192.167.1.1

OSPF: IETF GR Process grace-LSA from nbr 5.5.5.5 on VLink 192.167.1.1, age 1, grace period 200, graceful restart reason: Switch to redundant control processor, graceful ip address: 0.0.0.0

OSPF: IETF GR Enter graceful restart helper mode for nbr 5.5.5.5 on VLink 192.167.1.1 for 199 seconds (requested 200 sec)

OSPF: IETF GR Received grace-LSA from 5.5.5.5(addr: 192.167.1.1) on FastEthernet0/0

OSPF: IETF GR Validate grace-LSA from nbr 5.5.5.5 on FastEthernet0/0

OSPF: IETF GR Process grace-LSA from nbr 5.5.5.5 on FastEthernet0/0, age 1, grace period 200, graceful restart reason: Switch to redundant control processor, graceful ip address: 192.167.1.1

OSPF: IETF GR Enter graceful restart helper mode for nbr 5.5.5.5 on FastEthernet0/0 for 199 seconds (requested 200 sec)

OSPF: IETF GR Resynchronize with nbr 5.5.5.5(addr: 192.167.1.1)

OSPF: IETF GR Received grace-LSA from 5.5.5.5(addr: 192.167.1.1) on FastEthernet0/0

OSPF: IETF GR Validate grace-LSA from nbr 5.5.5.5 on FastEthernet0/0

OSPF: IETF GR Process grace-LSA from nbr 5.5.5.5 on FastEthernet0/0, age 3600, grace period 200, graceful restart reason: Switch to redundant control processor, graceful ip address: 192.167.1.1

OSPF: Recv MSG_OSPF_GR_HELP_RT_TERMINATE message

OSPF: IETF GR Exiting graceful restart helper mode for nbr 5.5.5.5(addr: 192.167.1.1) on VLink 192.167.1.1 with 21 secs remaining

OSPF: scheduling rtr lsa for area 0 process 1

OSPF: IETF GR Exiting graceful restart helper mode for nbr 5.5.5.5(addr: 192.167.1.1) on FastEthernet0/0 with 21 secs remaining

OSPF: scheduling rtr lsa for area 1 process 1

OSPF: scheduling net lsa on intf FastEthernet0/0

61.18 debug ip ospf retransmission

Syntax

To display retransmission of OSPF paceket, uset the debug ip ospf retransmission command

debug ip ospf retransmission

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display transmission processo OSPF packets

Example

Switch# debug ip ospf retransmission

OSPF: retransmit UPDATE to 192.168.40.3 (RID 192.168.40.3), state FULL

……

61.19 debug ip ospf spf

Syntax

To display information of SPF algorithm, use the following commands

debug ip ospf spf

debug ip ospf spf intra

debug ip ospf spf inter

debug ip ospf spf external

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

The debug ip ospf spf statistic command displays the OSPF routes calculation process

Example

Switch # debug ip ospf spf

OSPF[1]: too soon to run SPF, or SPF already scheduled

OSPF[1]: run ospf_spf_run for area 0

OSPF[1]: start doing SPF for AREA 0, RTAB_REV(ospf) 2

OSPF: Initializing to do SPF

OSPF[1]: SPF Area 0 running Router LSA

OSPF[1]: ospf_nh_find: 192.85.1.1

OSPF[1]: Area(0) add LSA(192.85.1.5, LS_NET) 1 under LSA(192.85.1.1, LS_RTR)

OSPF: ospf_rtr_netbacklink is called

OSPF[1]: ospf_nh_add 192.85.1.5

OSPF[1]: Area(0) add LSA(192.85.1.5, LS_RTR) 1 under LSA(192.85.1.5, LS_NET)

OSPF: ospf_rtr_netbacklink is called

OSPF[1]: ospf_nh_add 192.85.1.4

……

OSPF[1]: ospf_update_local_table, DEST 192.85.1.0, MASK 255.255.255.0, OSPF_REV 2, calc in area 0, AREA_REV 2

OSPF[1]: info REV 1, LS_TYPE 0, redorded in area 0, AREA_REV 2, state 12

OSPF[1]: info REV 2, LS_TYPE 2, redorded in area 0, AREA_REV 2, state 1

OSPF[1]: end doing SPF for AREA 0

OSPF[1]: finish ospf_spf_run for area 0 with err_code 0

OSPF[1]: ospf_add_main_table

OSPF[1]: delete route 192.85.1.0 first (255.255.255.0).

OSPF[1]: ospf_create_main_table_route equi_lsdb_num=1 maximum_paths=8

OSPF[1]: ospf_create_main_table_route RT 192.85.1.0 LS_TYPE 2 nh 192.85.1.1 area 0.0.0.0

OSPF[1]: build route 192.85.1.0/24 nh num=1, state=0x00031000

Description of the displaying fields:

Field	Description
LSA(192.85.1.5, LS_NET)	ID and type of LSA

61.20 debug ip ospf tree

Syntax

To display establishment of SPF tree of OSPF, use the debug ip ospf tree

debug ip ospf tree

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display establishment of SPF tree of OSPF from the output of this command

Example

Switch # debug ip ospf tree

OSPF[1]: Area(0) add LSA(192.85.1.1, LS_NET) 1 under LSA(192.85.1.1, LS_RTR)

OSPF[1]: Area(0) add LSA(1.1.1.1, LS_RTR) 1 under LSA(192.85.1.1, LS_NET)

OSPF[1]: Area(0) add LSA(192.85.1.5, LS_RTR) 1 under LSA(192.85.1.1, LS_NET)

OSPF[1]: Area(0) add LSA(1.0.4.1, LS_SUM_NET) 2 under LSA(1.1.1.1, LS_RTR)

OSPF[1]: Area(0) add LSA(56.0.0.1, LS_SUM_NET) 2 under LSA(1.1.1.1, LS_RTR)

OSPF[1]: Area(0) add LSA(11.1.1.1, LS_SUM_NET) 2 under LSA(1.1.1.1, LS_RTR)

OSPF[1]: call ospf_update_local_table_BFS

Description of the displaying fields:

Field	Description
LSA(1.0.4.1, LS_SUM_NET)	ID and type of LSA
add	Sub-LSA
under	parent LSA

61.21 default-information originate

Syntax

To generate a default route into an Open Shortest Path Firstly (OSPF) routing domain, use the **default-information originate** command

default-information originate [**always** | **metric-type** [*1* | *2*] | **metric** *cost* | **route-map** *map-name*]

no default-information originate

Parameter

parameter	description
originate	Generate a default external route into an Open Shortest Path Firstly (OSPF) routing domain
Always	(Optional) Always advertises the default route regardless of whether the software has a default route
metric-type [*1*	*2*]	(Optional) Metric value type. The value ranges from 1 to 2. The default value is 2
metric *cost*	(Optional) The routing cost value ranges from 0 to 16777214, and the default value is 100
route-map map-name	(Optional) Routing process will generate the default route if the route map is satisfied

Default value

This command is disabled by default

Command mode

router configuration

Usage guidelines

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPF routing domain, the software automatically becomes an Autonomous System Boundary Router Switch. However, an ASBR Switch does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have

specified the always keyword

When you use this command for the OSPF process, you must satisfy the route-map argument. Use the **default-information originate always route-map** command when you do not want the dependency on the default network in the routing table

Example

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

!

router ospf 109

default-information originate metric-type 1

redistribute rip 1

!

Related commands

Redistribute

61.22 default-metric

Syntax

To set default metric values for the Open Shortest Path Firstly (OSPF) routing protocol, use the default-metric command. To return to the default state, use the no form of this command

default-metric *value*

no default-metric

Parameter

parameter	description
value	Default metric value appropriate for the specified routing protocol, in the range 1~16777214

Default value

Default metric value is 10

Command mode

OSPF Routing configuration mode

Usage guidelines

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed

Example

The example assigns 3 as the default metric routes

Switch_config_ospf_100#default-metric 3

Related commands

redistribute

61.23 distance

Syntax

To set the management distance based on the router-id of inform route and of ospf route set by the destination segment, run the following command. To return to the default setting, use the no form of this command.

distance *value* [*network mask] [access-list-name]*

no distance *value* [*network mask]*

Parameter

Parameter	Description
value	(Optional) management distance. The value ranges from 1 to 255
network	(Optional) The segment which router-id of the inform router locates
mask	(Optional) The segment mask which router-id of the inform router locates
access-list-name	(Optional) Name of the access list

Default value

intra-area: 110

inter-area: 110

external: 150

Command mode

OSPF Routing configuration mode

Usage guidelines

At least there is a parameter

The command works the same with command "distance ospf". While this command can set a finer management distance according to router-id of the inform router and destination segment

Example

The following example shows how to set the management distance of the route complying with the list bd

which sent by router 1.1.1.1. as 100:

!

router ospf 1

distance 100 1.1.1.1 255.255.255.255 bd

redistribute ospf 2

!

Related command

distance ospf

61.24 distance ospf

Syntax

To define Open Shortest Path Firstly (OSPF) route administrative distances based on route type, use the distance ospf command To restore the default value, use the no form of this command

distance ospf {[**intra-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}

no distance ospf [**intra-area**] [**inter-area**] [**external**]

Parameter

parameter	description
intra-area dist1	(Optional) Sets the distance for routes in an area, learned by redistribution. The default value is 110
inter-area dist2	(Optional) Sets the distance for all routes from one area to another area. The default value is 110
external dist3	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 150

Default value

intra-area: 110

inter-area: 110

external: 150

Command mode

OSPF Routing configuration mode

Usage guidelines

There is at least one parameter

This command performs the same function as the distance command used with an access list. However, the distance ospf command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list

Example

The following example changes the external distance to 200:

Switch A:

```
!
router ospf 1
 distance ospf external 200
 redistribute ospf 2
!
router ospf 2
 distance ospf external 200
 redistribute ospf 1
!
```

Switch B:

```
!
router ospf 1
 distance ospf external 200
 redistribute ospf 2
!
router ospf 2
 distance ospf external 200
 redistribute ospf 1
!
```

Related commands

distance

61.25 filter

Syntax

To configure routing fliter list, use the **filter** command. Use the no filter command to restore the default

filter {**interface-type** *interface*-number | *****} **in** {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

no filter {**interface-type** *interface*-number | *****} **in**

Parameter

parameter	description
***interface*-type**	Interface type
interface-number	Interface number
*	All interfaces
In	Filters incoming ospf routes
access-list-name	Name of access list
access-list-name	Name of access list
prefix-list-name	Name of prefix list

Default value

none

Command mode

OSPF Routing configuration mode

Usage guidelines

none

Example

Switch_config_ospf_1#filter * in access-list mylist

61.26 graceful-restart

Syntax

To set OSPF graceful restart and related parameters, run the following command. To return to the default setting, use the no form of this command

graceful-restart { **ietf [helper {disable | strict-lsa-checking }]** | **interval** *period* }

no graceful-restart { **ietf [helper {disable | strict-lsa-checking }]** | **interval** }

Parameter

Parameter	Description
ietf	Enables graceful restart of IETF standard (based on rfc 3623). The command is disabled by default.

interval *period*	Configures the time limit of graceful restart. The value ranges from 40~1800s. The default value is 120s
helper disable	(Optional) Disable GR helper. By default, the device can be GR helper of any OSPF neighbor
helper strict-lsa-checking	(Optional) Enable strict-lsa-checking. When GR Helper detects the change of LSA, exit from Help mode. The command is disabled by default

Default value

None

Command mode

OSPF Routing configuration mode

Usage guidelines

None

Example

```
!
router ospf 1
 router-id 192.85.1.1
 network 192.85.1.0 255.255.255.0 area 0
 graceful-restart ietf
 graceful-restart interval 90
!
```

61.27 ip ospf authentication

Syntax

To designate the authentication mode of an interface receiving and sending ospf packets, run the following command. To return to the default setting, use the no form of this command

ip ospf authentication { **simple | message-digest** }

no ip ospf authentication

Parameter

Parameter	Description
simple	Authentication information verified by the plaintext

message-digest	Authentication information verified by MD5

Default value

No authentication

Command mode

Interface configuration mode

Usage guidelines

If use the command "**ip ospf authentication simple**" to verify the interface with the plaintext, you must configure a plaintext password with the command "**ip ospf password**". If use the command "**ip ospf authentication message-digest**" to designate the specified interface with md5 encryption authentication, you must configure md5 key with the command "**ip ospf message-digest-key**". If in one network, all OSPF are guaranteed with OSPF mutual communication, they must share the same verification type and passwords

Considering the compatibility, the authentication type of one ospf domain must be kept. If no ospf authentication type is configured on the interface, the authentication type of the domain which the interface belongs to will be used (The default authentication type is no authentication.)

Example

The following example shows how to verify interface VLAN 2 with md5 verification.

```
!
interface VLAN2
 ip address 131.119.251.201 255.255.255.0
 no ip directed-broadcast
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 abcdefg
!
router ospf 1
 network 131.119.0.0 255.255.0.0 area 0
!
```

Related command

ip ospf password

ip ospf message-digest-key

area authentication

61.28 ip ospf bfd

Syntax

To enable BFD fast check function in the routing configuration mode, run the following command

ip ospf bfd

To return to the default setting, use the no form of this command

ip ospf bfd [disable]

To disable interface bfd, run the following command

no ip ospf bfd

Parameter

disable: disable the function of bfd on the interface

Default value

No bfd

Command mode

Interface configuration mode

Usage guidelines

This function enables ospf and bfd collaborating to detect change of the fast detection link status

Example

The following example shows how to enable bfd collaboration on the interface vlan2:

```
!
interface VLAN2
 ip address 172.16.0.1 255.255.0.0
 no ip directed-broadcast
 ip ospf bfd
!
router ospf 110
 network 172.16.0.0 255.255.0.0 area 1
!
```

Related command

bfd all-interfaces

61.29 ip ospf cost

Syntax

To specify the cost of OSPF protocol on an interface, use the ip ospf cost command in interface configuration mode. To restore to the default value, use the no form of this command

ip ospf cost *cost*

no ip ospf cost

Parameter

parameter	description
cost	the cost of OSPF protocol. It can be a value in the range from 1 to 65535

Default value

Default value of the OSPF protocol cost depends on rate of the interface

Command mode

interface configuration mode

Example

The following example sets the interface cost value to 2:

Switch_config_v2#ip ospf cost 2

specify the the interface cost of OSPF protocol, to restore the default value,use the no ip ospf command

61.30 ip ospf dead-interval

Syntax

To set the dead-interval of specified routing switch in neighbourhood, use the ip ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameter

parameter	description
Seconds	Interval (in seconds) of specified routing switch in neighbourhood. The range is 1 to 2147483647

Default value

40 seconds

Command mode

interface configuration

Usage guidelines

The dead interval is advertised in OSPF hello packets and sent with OSPF hello packets. This value must be the same for all networking devices on a specific network and four times the interval set by the ip ospf hello-interval command

Example

The following example sets the OSPF dead interval to 60 seconds:

Switch_config_v2#ip ospf dead-interval 60

Related commands

ip ospf hello-interval

61.31 ip ospf demand-circuit

Syntax

To designate the interface as the demand circuit, run the following command. To return to the default setting, use the no form of this command

ip ospf demand-circuit

no ip ospf demand-circuit

Parameter

None

Default value

Disabled

Command mode

Interface configuration mode

Usage guidelines

After configuring the on-demand circuit, hello packets and periodically link status update packets can be suppressed. The bottom link can be disabled after the network topology is stable

Example

The following example shows how to configure interface VLAN2 as on-demand circuit

Switch_config_v2#ip ospf demand-circuit

61.32 ip ospf hello-interval

Syntax

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the ip ospf hello-interval command. To return to the default value, use the no form of this command

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter

parameter	description
Seconds	Specifies the interval (in seconds)of sending hello packets. The range is from 1 to 65535

Default value

10 seconds

Command mode

interface configuration mode

Usage guidelines

This value is advertised in the hello packets and sent with the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network

Example

The following example sets the interval between hello packets to 20 seconds:

Switch_config_v2#ip ospf hello-interval 20

Related commands

ip ospf dead-interval

61.33 ip ospf message-digest-key

Syntax

To enable Open Shortest Path Firstly (OSPF) Message Digest 5 (MD5) authentication, use the ip ospf message-digest-key md5 command. To remove an old MD5 key, use the no form of this command

ip ospf message-digest-key *keyid* **md5** [*0* | *7*] *key*

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

Parameter

parameter	description
keyid	An identifier in the range from 1 to 255
key	Alphanumeric password of up to 16 bytes
0	*7*	Designate the key type: plaintext (0) or ciphertext (7)

Default value

OSPF MD5 authentication is disabled

Command mode

interface configuration mode

Usage guidelines

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value

The process of changing keys is as follows. Suppose the current configuration is as follows:

!

interface VLAN2

no ip address

no ip directed-broadcast

ip ospf message-digest-key 100 md5 0 OLD

!

You change the configuration to the following:

!

interface VLAN2

no ip address

no ip directed-broadcast

ip ospf message-digest-key 100 md5 0 OLD

ip ospf message-digest-key 101 md5 NEW

!

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet - he first one authenticated by key 100 and the second one authenticated by key 101

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

interface VLAN2

no ip ospf message-digest-key 100

Then, only key 101 is used for authentication on Ethernet VLAN2

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover

Example

The following example sets a new key 19 with the password 8ry4222:

!

interface VLAN2

ip ospf message-digest-key 10 md5 0 xvv560qle

ip ospf message-digest-key 19 md5 0 8ry4222

!

Related commands

area authentication

61.34 ip ospf mib-binding

Syntax

To set OSPF progress of mib, run the following command. To return to the default setting, use the no form of this command

ip ospf mib-binding *process-id*

no ip ospf mib-binding

Parameter

Parameter	Description
process-id	OSPF process ID. The value ranges from 1 to 65535

Default value

MIB operation binds on OSPF with the most small progress

Command mode

Global configuration mode

Usage guidelines

When multiple OSPF progresses are configured, the command can be used to bind MIB with a specific OSPF progress

Example

The following example shows how to bind MIB operation to OSPF 100:

Switch_config#ip ospf mib-binding 100

61.35 ip ospf network

Syntax

To configure the Open Shortest Path Firstly (OSPF) network type, use the ip ospf network command. To return to the default value, use the no form of this command

ip ospf network { **broadcast** | **non-broadcast** | **point_to_multipoint** [**broadcast** | **non-broadcast**]| **point-to-point**}

no ip ospf network

Parameter

parameter	description
broadcast	Sets the network type to broadcast
nonbroadcast	Sets the network type to nonbroadcast multiaccess
point-to-point	Sets the network type to point-to-point
point-to-multipoint	Sets the network type to point-to-multipoint

Command mode

interface configuration mode

Usage guidelines

Using this feature, you can configure broadcast networks as NBMA networks. Configuring NBMA networks as point-to-multipoint network if there is no assurance to direct connection between any two routing switches

Example

The following example sets VLAN2 as a nonbroadcast network type:

Switch_config_v2#ip ospf network non-broadcast

61.36 ip ospf passive

Syntax

To cancel sending a HELLO packets on an interface, use the ip ospf passive command. Use the no form of this command to reactivate the sending of HELLO packet

ip ospf passive

no ip ospf passive

Parameter

This command has no keywords or parameters

Default value

Send HELLO packets on the interface

Command mode

interface configruration mode

Usage guidelines

If you cancel sending a HELLO packet on an interface, a specified subnetwork wll keep on declaring to other interfaces, and the routing update from other routing switch to this interface can still be received and dealt with. This is usually applicable to the STUB network, for in this kind of network there is usually no other OSPF routing switches

Example

The following example sends a HELLO packet to all interfaces(except for VLAN2) overridden by network 172.16.0.0:

```
!
interface VLAN2
 ip address 172.16.0.1 255.255.0.0
 no ip directed-broadcast
 ip ospf passive
!
router ospf 110
 network 172.16.0.0 255.255.0.0 area 1
!
```

Related commands

None

61.37 ip ospf password

Syntax

To configure password for a neighbor route, use the ip ospf password command. Use the no form of this command to cancel the configuration

ip ospf password [*0* | *7*] *password*

no ip ospf password

Parameter

parameter	description
password	Any consecutive 8-digit character string
0	*7*	Designate the key type: plaintext (0) or ciphertext (7)

Default value

No password is predefined by default

Command mode

Interface configuration mode

Usage guidelines

The password generated by this command directly inserts OSPF information packet. This command can configure one password for each network of each interface. All neighbor routers must have the same password to exchange OSPD routing information

When the configured key is displayed, it will be displayed as plain text or cipher text according to the global command

Example

ip ospf password yourpsw

Related commands

area authentication

61.38 ip ospf priority

Syntax

To set the router priority, use the ip ospf priority command. To return to the default value, use the no form of this command

ip ospf priority *priority*

no ip ospf priority

Parameter

parameter	description
priority	specifies the priority. The range is from 0 to 255

Default value

Priority of 1

Command mode

interface configuration mode

Usage guidelines

When two routing switches attached to a network both attempt to become the designated routing switch, the one with the higher routing switch priority takes precedence. If there is a tie, the routing switch with the higher

routing switch ID takes precedence. A routing switch with a routing switch priority set to zero is ineligible to become the designated routing switch or backup designated routing switch. routing switch priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks)

Example

The following example sets the routing switch priority value of VLAN2 to 8:

Switch_config_v2#ip ospf priority 8

Related commands

neighbor

61.39 ip ospf retransmit-interval

Syntax

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the ip ospf retransmit-interval command. To return to the default value, use the no form of this command

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Parameter

parameter	description
seconds	Time (in seconds) between retransmissions. The range is from 1 to 3600 seconds

Default value

The default is 5 seconds

Command mode

interface configuration mode

Usage guidelines

When a routing switch sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the routing switch receives no acknowledgment, it will resend the LSA. The setting of the seconds argument should be greater than the expected round-trip delay between any two routing switches on the attached network

Example

The following example sets the retransmit interval value to 8 seconds:

Switch_config_v2#ip ospf retransmit-interval 8

61.40 ip ospf transmit-delay

Syntax

To set ip ospf transmit-delay time on the interface, run the following command. To return to the default setting, use the no form of this command

ip ospf transmit-delay *time*

no ip ospf transmit-delay

Parameter

Parameter	Description
time	ip ospf transmit-delay time Unit:s, the value ranges from 1 to 3600

Default value

1s

Command mode

Interface configuration mode

Example

The following example shows how to configure the transmit-delay time on interface VLAN2 as 3s

Switch_config_v2#ip ospf transmit-delay 3

61.41 ip ospf mtu-ignore

Syntax

To set the port to not check the mtu value in the message, use **ip ospf mtu-ignor** command. Use no form of the command to restore the default settings

ip ospf mtu-ignore

no ip ospf mtu-ignore

Default

The default state of the interface is to check the mtu value in the packet

Command mode

Interface configuration mode

Example

The following example shows how to configure not to check the mtu value on interface VLAN2

Switch_config_v2#ip ospf mtu-ignore

61.42 limit max-ext-lsa

Syntax

To set max amount of AS external LSA, run the following command. To return to the default setting, use the no form of this command

limit max-ext-lsa *value*

no limit max-ext-lsa

Parameter

Parameter	Description
value	Max amount of AS external LSA. The value ranges from 0 to 1000000

Default value

No limit to the max amount of AS external LSA

Command mode

OSPF Routing configuration mode

Usage guidelines

The command is used to set all routes in OSPF autonomous domain as the same value

Example

To set max amount of AS external LSA in OSPF progress 100 to be 1000:

Switch_config#router ospf 100

Switch_config _ospf_100#limit max-ext-lsa 1000

61.43 limit retransmissions

Syntax

To set the max re-transmit times of ospf, run the following command. The re-transmit packets are DD, REQ and LSU. To return to the default setting, use the no form of this command

limit retransmissions { *timers* **| disable }**

no limit retransmissions [dsiable]

Parameter

Parameter	Description
timers	Max re-transmit times (The default value is 25)
disable	Cancel the max re-transmit times (No limit to the re-transmit)

Default value

The default re-transmit times is 25

Command mode

OSPF Routing configuration mode

Usage guidelines

None

Example

The following example shows how to modify the retransmit times to 10:

Switch_config_ospf_100#limit retransmissions 10

The following example shows how to restart the retransmit times without limit:

Switch_config_ospf_100#limit retransmissions disable

61.44 maximum-paths

Syntax

To set the max amount of next hop of the equivalent route, run the following command. To return to the default setting, use the no form of this command

maximum-paths *value*

no maximum-paths

Parameter

Parameter	Description
value	The max amount of next hop of the equivalent route. The value ranges from 1 to 8

Default value

8

Command mode

OSPF Routing configuration mode

Usage guidelines

If the value is 1, the load distribution does not work

Example

The following example shows how to set next hop of the equivalent route in OSPF progress 100 to be 3

Switch_config#router ospf 100

Switch_config_ospf_100#maximum-paths 3

61.45 neighbor

Syntax

To configure Open Shortest Path Firstly (OSPF) routing switch interconnecting to nonbroadcast networks, use the neighbor command. To remove a configuration, use the no form of this command

neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*]

no neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [*cost number*]

Parameter

parameter	description
ip-address	Interface IP address of the neighbor
priority number	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces
poll-interval seconds	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces
cost number	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the number argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks

Default value

no default value

Command mode

OSPF routing configuration

Usage guidelines

In X.25 and Frame Relay networks you can configure OSPF to run as a broadcast network. Detailed information is as follow:

In X.25 and frame relay map

One nonbroadcast network neighbor must be configured in the routing switch. The neighbor address must be on the primary address of the interface

If a neighboring router has become inactive, it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called Poll Interval

When the routing switch first starts up, it sends only hello packets to those routing switches with nonzero priority, that is, routing switches that are eligible to become designated routeing switch (DRs) and backup designated routing switches (BDRs). After the DRs and BDRsare selected, DRs and BDRs will then start sending hello packets to all neighbors in order to form adjacencies

Example

The following example declares a routing switch at address 131.108.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
!
router ospf 100
 neighbor 131.108.3.4 priority 1 poll-interval 180
!
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
!
interface VLAN2
 ip address 10.0.1.1 255.255.255.0
 no ip directed-broadcast
 ip ospf network point-to-multipoint non-broadcast
!
!
router ospf 1
 network 10.0.1.0 255.255.255.0 area 0
 neighbor 10.0.1.3 cost 5
 neighbor 10.0.1.4 cost 10
 neighbor 10.0.1.5 cost 15
!
```

Related commands

ip ospf priority

61.46 network area

Syntax

To define several network segments in an area as a network range, use the network area command. To disable the feature, use the no form of this command

network *network mask* **area** *area_id*

no network *network mask* **area** *area_id*

Parameter

parameter	description
network	Network Ip address, in dotted decimal format
mask	Mask, in dotted decimal format
area_id	Id of area

Default value

This command is disabled by default

Command mode

OSPF Routing configuration mode

Usage guidelines

Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the network command list and ignore the subsequent overlapping portions. Importing network range and specifying the range can reduce the switch state of routing information among areas

Example

The following example defines network range 10.0.0.0 255.0.0.0 and adds to area 2:

Switch_config_ospf_2#network 10.0.0.0 255.0.0.0 area 2

61.47 redistribute

Syntax

To configure OSPF to redistribute routes of other routing protocols, use the redistribute command. Use the no form of this command to restore the default

redistribute *protocol process-id* [**metric-type** [*1* | *2*] | **metric** *cost* | **tag** *tag* | **route-map** *WORD*]

no redistribute *protocol process-id* [**metric | tag | route-map**]

Parameter

parameter	Description
protocol	Redistributes former protocols that learned, it should be one of the following: beigrp, bgp, connect, isis, ospf, rip, static
process-id	(Optional) Autonomous system number. There is no parameter for connect, static
metric-type [*1*	*2*]	(Optional) Metric value type. The value ranges from 1 to 2. The default value is 2
metric *cost*	(Optional) The routing cost value, ranges from 0 to 16777214, and the default value is 100

tag *tag*	(Optional) The routing tag in the external LSA, in the range of 0 to 4294967295. The default value is 0
route-map *WORD*	(Optional) Configure the route conforming to the specified routing policy

Default value

Enabled

Command mode

OSPF Routing configuration mode

Usage guidelines

External route refers to the route to the outside of the autonomous system. This command does not redistribute the default route

Example

The following example redistributes static route, metric value is Type-1, a route tag is 1000, and a metric value is 10:

Switch_config_ospf_2#redistribute static metric-type 1 tag 1000 metric 10

61.48 restart ospf

Syntax

To restart the OSPF process, use the restart ospf command. If no process-id is specified, all OSPF processes are restarted

restart ospf [*process-id*] [**graceful**]

Parameter

parameter	description
process-id	The number of OSPF process. Range is from 1 to 65535
graceful	(Optional) Restart OSPF process gracefully without changing Router ID

Default value

None

Command mode

EXEC

Usage guidelines

Use **restart ospf [process-id]** command to restart the OSPF process, you can get the following results:

(1) You can immediately clear all data structures of the OSPF process

(2) This command will reselect the Router ID

(3) The OSPF configuration before restarting will not be lost

If you restart gracefully, you can achieve uninterrupted forwarding, and the Router ID before and after the restart remains unchanged

Example

Restart all OSPF processes gracefully:

restart ospf graceful

61.49 router-id

Syntax

To designate router-id in OSPF in progesss, run the following command. To return to the default setting, use the no form of this command

router-id *ip-address*

no router-id

Parameter

Parameter	Description
ip-address	Router ID of OSPF progress. Point spread decimalism

Default value

OSPF progress selects router-id on its own

Command mode

OSPF Routing configuration mode

Usage guidelines

After configuring the new router-id, the OSPF progress will be restarted. The configured router-id is exclusive to the whole OSPF autonomous domain

Example

The following example shows how to configure one OSPF progress and the designated router-id is 1.1.1.1:

```
!
router ospf 109
 router-id 1.1.1.1
!
```

Related command

router ospf

61.50 router ospf

Syntax

To configure an Open Shortest Path Firstly (OSPF) routing process, use the router ospf command. To terminate an OSPF routing process, use the no form of this command

router ospf *process-id* [**vrf** *WORD*]

no router ospf *process-id* [**vrf** *WORD*]

Parameter

parameter	description
process-id	ospf process ID. The value ranges from 1 to 65535
vrf *WORD*	(Optional) Configure the name of the VPN instance bound to the OSPF process

Default value

No OSPF routing process is defined

Command mode

Global configuration mode

Usage guidelines

You can specify multiple OSPF routing processes in each router

On a router, you can run multiple ospf processes by specifying different process numbers. In this case, you can use the router-id command to specify different Router IDs for different processes

If OSPF is used as a VPN internal routing protocol, you need to bind the OSPF process to the VPN instance

Example

The following example configures an OSPF routing process and assign a process number of 109:

router ospf 109

Related commands

network area

61.51 show ip ospf

Syntax

To display general information about Open Shortest Path Firstly (OSPF), use the show ip ospf command

show ip ospf [*process-id*]

Parameter

parameter	description
process-id	(Optional) Process ID

Default value

none

Command mode

EXEC

Usage guidelines

Troubleshoot OSPF problems according to the output of this command. To display only the global configuration information of the corresponding OSPF process if configured with the process-id parameter

Example

The following display the configuration information of OSPF process :

Switch#show ip ospf

OSPF process: 1, Router ID is 192.168.99.81

Distance: intra-area 110 inter-area 130 external 150

Source Distance Access-list

240.240.1.1/24 1 what

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Number of areas is 3

AREA: 1

Number of interface in this area is 1(UP: 1)

Area authentication type: None

AREA: 36.0.0.1

This is a stub area.

Number of interface in this area is 0(UP: 0)

Area authentication type: None

AREA: 192.168.20.0

Number of interface in this area is 0(UP: 0)

Area authentication type: None

Net Range list:

10.0.0.0/255.0.0.0 Not-Advertise

140.140.0.0/255.255.0.0 Advertise

filter list on receiving UPDATE is Gateway: weewe

filter list on sending UPDATE is Prefix: trtwd

Summary-address list:

150.150.0.0/16 advertise

Switch#

Description of the displaying fields

field	description
OSPF process: 1	OSPF process ID
Router ID is 192.168.99.81	Routing switch ID
Distance: intra-area 110 inter-area 130 external 150	The default administrative distance that the current routing switch adopts
Source Distance Access-list	Administrative distance based on concrete routing configuration
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs	Value of two timer related to OSPF
Number of areas is 3	The number of the field that currently configured and the parameter configured in each field
filter list on receiving...	The configured filter list on receiving routes
filter list on sending	The configured filter list on sending routes
Summary-address list	The configured routing summary address

61.52 show ip ospf border-routers

Syntax

To display the internal Open Shortest Path Firstly (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the show ip ospf border-routers command

show ip ospf border-routers

Parameter

none

Default value

none

Command mode

EXEC

Example

Switch #

Switch #show ip ospf border-routers

OSPF process: 1

Codes: i - Intra-area route, I - Inter-area route

Destination Adv-Rtr Cost Type Area

i 192.168.20.77 192.168.20.77 11 ABR 0

Switch #

Field description:

field	description
Destination	Routing switch ID of the destination
Adv-Rtr	Next hop toward the destination
Cost	Cost of using this route
Type	The routing switch type of the destination; it is either an ABR or ASBR or both
Area	The area ID of the area from which this route is learned

61.53 show ip ospf database

Syntax

To display lists of information related to the Open Shortest Path Firstly (OSPF) database, use the show ip ospf database command

show ip ospf database

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

Display lists of information related to the Open Shortest Path Firstly (OSPF) database in accordance with debugging information of the command, and it is helpful for users in troubleshooting

Example

Switch #show ip ospf database

OSPF process: 1

(Router ID 192.168.99.81)

AREA: 0

Router Link States

Link ID ADV Router Age Seq # Checksum Link count

192.168.20.77 192.168.20.77 77 0x8000008a 0x90ed 1

192.168.99.81 192.168.99.81 66 0x80000003 0xd978 1

Net Link States

Link ID ADV Router Age Seq # Checksum

192.168.20.77 192.168.20.77 80 0x80000001 0x9625

Summary Net Link States

Link ID ADV Router Age Seq # Checksum

192.168.99.0 192.168.99.81 87 0x80000003 0xd78c

AREA: 1

Router Link States

Link ID ADV Router Age Seq # Checksum Link count

192.168.99.81 192.168.99.81 70 0x80000002 0x0817 1

Summary Net Link States

Link ID ADV Router Age Seq # Checksum

192.168.20.0 192.168.99.81 66 0x80000006 0xd1c1

Switch #

Field description:

field	Description
AREA: 1	OSPF area

Router Link States/Net Link States/Summary Net Link States	LSA type
Link ID	LSA ID
ADV Router	Advertising routing switch's ID
Age	Link state age
Seq #	Link state sequence number
Checksum	Fletcher checksum of the complete contents of the link state advertisement

61.54 show ip ospf interface

Syntax

To display Open Shortest Path Firstly (OSPF)-related interface information, use the show ip ospf interface command

show ip ospf interface

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display configuration and operation situation of OSPF on an interface according to the debugging information of this command. Users can confirm whether the configuration is right or not and it is helpful in troubeshooting

Example

Switch #show ip ospf interface

VLAN1 is up, line protocol is up

Internet Address: 10.0.1.1/24

Interface index: 34, 0x4057ea8

Nettype: Point-to-MultiPoint with Non-Broadcast

OSPF process is 1, AREA: 0, Router ID: 192.168.30.81

Cost: 1, Priority 1, Transmit Delay is 1 sec

Hello interval is 30, Dead timer is 120, Retransmit is 5

OSPF INTF State is IPOINT_TO_MPOINT

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 1.0.4.1

Null authentication enabled

Switch #

Displaying field description:

field	description
Internet Address:	Interface IP address
Nettype	Net type of OSPF interface
OSPF process is	OSPF process number
AREA	OSPF area.
Router ID	Routing switch ID
Cost	Cost of routing switch OSPF interface
Transmit Delay is	Transmit delay
Priority	Priority of routing switch interface
Hello interval	Number of seconds until next hello packet is sent out this interface.
Dead timer	Dead timer
Retransmit	Retransmit interval
OSPF INTF State is	OSPF nterface state

61.55 show ip ospf neighbor

Syntax

To display Open Shortest Path Firstly (OSPF)-neighbor information, use the show ip ospf neighbor command

show ip ospf neighbor [detail]

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display neighbor situation of OSPF from the output of this command to help user troubleshoot OSPF

Example

Switch#show ip ospf neighbor

AREA: 0

Neighbor ID Pri State DeadTime Neighbor Addr Interface

1.0.4.1 0 FULL/- 100 10.0.1.3 VLAN1

Displaying field description:

field	description
OSPF process	OSPF process number
AREA	OSPF area
Neighbor	Neighbor routing switch ID
Pri	Routing switch priority of the neighbor, neighbor state
State	OSPF state
DeadTime	Expected time before software will declare the neighbor dead
Neighbor Addr	Neighbor ip address
Interface	Interface to which connects the neighbor

61.56 show ip ospf virtual-link

Syntax

To display information of Open Shortest Path Firstly (OSPF) virtual links, use the show ip ospf virtual-links command

show ip ospf virtual-link

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

The information displayed by the show ip ospf virtual-links command is useful in debugging OSPF routing operations. To display the detailed information of adjacency relation of the OSPF neighbour, use the show show ip ospf neighbour command

Example

Switch#show ip ospf vir

Virtual Link Neighbor ID 200.200.200.2 (UP)

Run as Demand-Circuit

TransArea: 1, Cost is 185

Hello interval is 10, Dead timer is 40 Retransmit is 5

INTF Adjacency state is IPOINT_TO_POINT

Description of the displaying fields:

field	description
neibhbor ID	The configured neighbor ID of the remote side
neighbour state	Adjacency relation of the OSPF neighbor
Demand-Circuit	Indicates working under DC mode
TransArea	The transit area through which the virtual link is formed
cost	The cost of reaching the OSPF neighbor through the virtual link
Hello Interval	The current Hello interval
DeadTime	Expected time before software will declare the neighbor dead
Retrans	Retransmit interval
INTF Adjacency State	The state of virtual link

Related commands

area vritual-link

show ip ospf neighbor

61.57 stub-router

Syntax

To set stub route, rrun the following command. To return to the default setting, use the no form of this command

stub-router

no stub-router

Parameter

None

Default value

Disabled

Command mode

OSPF Routing configuration mode

Usage guidelines

After the router is configured as Stub router, the router will not forward packets whose destination segment is not in the router. At the moment, in Router-LSA published by the router, the value of the link whose type is 1 (point to point link), 1(connecting to the transmission network) and 4 (virtual link) will be set as 65535, while the value of the link 3 (connecting to Stub network) will not be changed. Thus, when other routers are working, if there is a smaller router with less cost in the destination address, the data will not be forwarded by this Stub router

Example

The following example shows how to configure Stub router as the local router:

router ospf 109

stub-router

61.58 summary-address

Syntax

To create aggregate addresses for Open Shortest Path Firstly (OSPF), use the summary-address command. To restore the default, use the no form of this command

summary-address *address mask* [**not-advertise | tag** *value*]

no summary-address *address mask*

Parameter

parameter	description
address	Summary address designated for a range of addresses
Mask	IP subnet mask used for the summary route
not-advertise	(Optional) Suppress match routes that creat LSA
tag	(Optional) Set route tag
value	Route tag value, the range is from 0 to 4294967295, the default is 0

Default value

none

Command mode

OSPF Routing configuration mode

Usage guidelines

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table

Using this command for OSPF causes an OSPF Autonomous System Boundary Routing switch (ASBRs) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the area range command for route summarization

Example

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement

summary-address 10.1.0.0 255.255.0.0

Related commands

area range

ip ospf password

ip ospf message-digest-key

61.59 timers delay-timer

Syntax

To specify the delay interval between OSPF receiving a topology structure variety and initializing a minimum route priority computation, use the **timers delay-timer** command. Use the no form of this command to resotre default value

timers delay-timer *spf-delay*

no timers delay-timer

Parameter

parameter	description
spf-delay	Delay between topology variety and computation commencement in seconds, from 0 to 65535. Default value is 5 seconds. If the value is 0, that indicates there is no delay, namely, once there is a variety, the commencement of computation immediately starts

Default value

spf-delay: 5 seconds

Command mode

OSPF Routing configuration mode

Usage guidelines

The less the configured time is, the quicker the response to network variety. But this will take up more processing time

Example

timers delay-timer 10

61.60 timers hold-timer

Syntax

To configure the interval between two continuous SPF computation, use the timers hold command. Use the no form of this command to restore the default value

timers hold-timer *spf-holdtime*

no timers hold-timer

Parameter

parameter	description
spf-holdtime	The minimum value between two continuous computation, in the range from 0 to 65535. The default value is 10 seconds; 0 means that there is no time difference between two consecutive calculations

Default value

spf-holdtime: 10 seconds

Command mode

OSPF Routing configuration mode

Usage guidelines

The less the configured time is, the quicker the response to network variety. But this will take up more processing time

Example

timers hold-timer 20

61.61 timers age-timer

Syntax

To set time interval of OSPF checking LSA database aging, run the following command. To return to the default setting, use the no form of this command

timers age-timer *agetime*

no timers age-timer

Parameter

Parameter	Description
agetime	Check lsa database every agetime

Default value

agetime: 60s

Command mode

OSPF Routing configuration mode

Usage guidelines

The smaller the time, the faster the database responds, but with more processer time

Example

timers age-timer 50

Chapter 62 BGP Configuration Commands

62.1 address-family ipv4

Syntax

To eneter bgp ipv4 address family mode, run the following command. To return to the default setting, use the no form of this command

address-family ipv4 {mdt | multicast | unicast | vrf} [name]

Parameter

Parameter	Description
mdt	Enters ipv4 mdt configuration mode. It is used for mvpn
multicast	Enters ipv4 multicast configuration mode. It is used for multicast rpf query
unicast	Enters ipv4 unicast configuration mode. It is used for ipv4 unicast
name	Configuration parameters of address-family ipv4 vrf, which means enter vpn configuration mode

Default value

None

Command mode

BGP configuration mode

Usage guidelines

Expand bgp configuration mode

Example

The following example shows how to activate neighbor 1.1.1.1 ipv4 mdt route inform

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1

 address-family ipv4 mdt
 neighbor 1.1.1.1 activate
 exit-address-family
```

Related command

exit-address-family

62.2 address-family ipv6

Syntax

To enter bgp ipv6 address family configuration mode, run the following command

address-family ipv6 {multicast | unicast}

Parameter

Parameter	Description
multicast	Enters the configuration mode of ipv6 multicast
unicast	Enters the configuration mode of ipv6 unicast

Default value

None

Command mode

BGP configuration mode

Usage guidelines

Expand bgp configuration mode

Example

The following example shows how to activate neighbor 1.1.1.1 ipv6 routing inform:

router bgp 1

bgp log-neighbor-changes

neighbor 1.1.1.1 remote-as 1

address-family ipv6

neighbor 1.1.1.1 activate

exit-address-family

Related command

exit-address-family

62.3 address-family vpnv4

Syntax

To enter bgp vpnv4 address family configuration mode, run the following command

address-family vpnv4

Parameter

None

Default value

None

Command mode

BGP configuration mode

Usage guidelines

Expand bgp configuration mode: used for l3vpn configuration environment. The configuration mode is often used in condition of PE-PE interconnection

Example

The following example shows how to activate neighbor 1.1.1.1 vpnv4 routing inform

router bgp 1

bgp log-neighbor-changes

neighbor 1.1.1.1 remote-as 1

address-family vpnv4

neighbor 1.1.1.1 activate

exit-address-family

Related command

exit-address-family

62.4 aggregate-address

Syntax

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the aggregate-address command in address family or routing switch configuration mode. To disable this function, use the no form of this command

aggregate-address A.B.C.D/n [as-set] [**summary-only**] [**attribute-map** *map-name*]

no aggregate-address A.B.C.D/n

Parameter

parameter	description

A.B.C.D/n	Aggregate network
as-set	Including AS set path attribute (AS-SET) of aggregated routes
summary-only	Filters all more-specific routes from updates
attribute-map	Name of the route map used to set the attribute of the aggregate route
map-name	Name of the route map

Default value

none

Command mode

BGP configuration mode

Usage guidelines

You can implement aggregate routing in BGP in three methods: first,dynamic implement routing by forwarding redistribute; second, static implement routing by network command; third, static implement routing by aggregate. The routing created in this way are local routing, which can be announced to other equivalent, but not implement local IP address table

The generation of aggregation routes is to reduce the number of routes in the routing table and increase the efficiency of route indexes and the stability of routes. BGP aggregation routes are performed in the BGP routing table, and aggregation routes are considered as locally generated routes and will not be added to the routes table. But they can be seen in the BGP routing table. The aggregate-address command with the same prefix will override the original configuration

Aggregation routes usually aggregate existing routes according to certain rules. The existence of this route depends on the status of the its source route. BGP aggregation routes rely on the routes with the same prefix and more precise routes in the BGP routing table. When there is at least one route with the same prefix or a more precise route in the BGP routing table, the aggregation route can be valid. When the aggregation route is valid, it can be displayed by show ip bgp command, with a *> mark. The aggregation route can suppress the source route, then it is marked with s

Without the as-set option, the as-path attribute formation of the aggregation route follows the following rules:

All entries that appear in as-sequence should appear in the summarized as-path;

All entries that appear in as-set must appear in at least one type of summarized as-path;

The longest identical entry in as-sequence is used as the summarized as-sequence;

The remaining entries are as-set.

With the as-set option, the as-path attribute of all existing routes appears in the as-path of the aggregate route as as-set

Using the **summary-only** option not only creates an aggregation route (for example, 193.*.*.*), but also suppresses more specific routes

Use the **attribute-map** option to modify the attributes of the route when generating an aggregate route

The maximum number of aggregate commands that can be configured is determined by the switch resources,

such as the configured RAM

Example

In the following example, an aggregate BGP address is created :

router bgp 5

aggregate-address 193.0.0.0/8

Related commands

route-map

62.5 bgp always-compare-med

Syntax

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the bgp always-compare-med command. To disallow the comparison, use the no form of this command

bgp always-compare-med

no bgp always-compare-med

Parameter

none

Default value

Not compare the MED for paths from neighbors in different autonomous systems

Command mode

BGP configuration mode

Usage guidelines

Generally speaking, when BGP selects routes, only two from the same autonomous system can compare MED. Using **bgp always-comapre-med** command can make BGP always compare MED, regardless of whether the route comes from the same autonomous system. This can change the route selection process

Example

The following example enables the function

router bgp 5

bgp always-compare-med

Related commands

bgp bestpath med

bgp deterministic-med

62.6 bgp asnotation dot

Syntax

To enable asdot mode, run the following command

bgp asnotation dot

no bgp asnotation dot

Parameter

None

Default value

asplain mode

Command mode

BGP configuration mode

Usage guidelines

The command is used to configure the display form of as. Only when as is greater than 65535 can it is displayed in the form of asdot. The command takes effect needs to activate **clear ip bgp ***

Example

The following example shows how to enable the function:

router bgp 100

bgp asnotation dot

Related command

route bgp

show ip bgp

62.7 bgp bestpath med

Syntax

To modify the process way of Border Gateway Protocol (BGP) on Multi Exit Discriminator (MED) attribute, use the **bgp bestpath med** command. To disable the feature, use the no form of this command

bgp bestpath med {**confed** | **missing-as-worst**}

no bgp bestpath med {**confed** | **missing-as-worst**}

Parameter

parameter	description
confed	Autonous system confederation MED comparison attrubute
missing-as-worst	(Optional) Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable

Default value

none

Command mode

BGP configuration mode

Usage guidelines

If the MED attribute of BGP route is not configured, the value of MED is always considered to be 0, that is the least value, which has the most priority. When configured with the missing-as-worst option, if the MED attribute of BGP route is not configured, the value of MED is always considered to be the most maximum value, which has the least priority

By default, the same routes advertised by different BGP switches within the same autonomous system are compared to MED, while within the same autonomous system alliance, the same routes advertised by different autonomous systems are not compared to MED. After t all the same routes advert he confed option is configured, this rule is modified to make ised within the same autonomous system alliance compare MED

Example

By default, the MED comparison between (100)and (200) doesn't occur for they are not the routes from the same sub-autonomous system. But the MED comparison occurs when configured with the bgp bestpath med confed command, for they come from the sub-autonomous system 100 and 200 respecitively in the autonomous system alliance

Related commands

bgp always-compare-med

bgp deterministic-med

62.8 bgp client-to-client reflection

Syntax

To enable or restore route reflection from a BGP route reflector to clients, use the bgp client-to-client reflection command. To disable client-to-client route reflection, use the no form of this command

bgp client-to-client reflection

no bgp client-to-client reflection

Parameter

none

Default value

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients

Command mode

BGP configuration mode

Usage guidelines

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the no bgp client-to-client reflection command to disable client-to-client reflection

Example

In the following example, the local routing switch is a route reflector, and the three neighbors are fully meshed, turn off client-to-client reflection

router bgp 5

neighbor 192..168.20.190 router-reflector-client

neighbor 192..168.20.191 router-reflector-client

neighbor 192..168.20.192 router-reflector-client

no bgp client-to-client reflection Related commands

neighbor route-reflector-client

bgp cluster-id

62.9 bgp cluster-id

Syntax

bgp cluster-id *cluster-id*

no bgp cluster-id [*cluster-id*]

Parameter

parameter	description
cluster-id	Cluster ID of this router acting as a route reflector, which can be a IP address or a number; maximum of 4 bytes.

Default value

The local routing switch ID of the route reflector is used as the cluster ID when no ID is specified or when the no form of this command is entered

Command mode

BGP configuration mode

Usage guidelines

Together, one or more route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the routing switch ID of the route reflector. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. This allows all route reflectors in the cluster must be configured with a 4-byte cluster ID to recognize updates from peers in the same cluster

When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors

Example

In the following example, the local routing switch is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster. Neighbor 198.92.70.24 is a route reflection client:

router bgp 5

neighbor 198.92.70.24 route-reflector-client

bgp cluster-id 50000

Related commands

neighbor route-reflector-client

show ip bgp summary

62.10 bgp confederation identifier

Syntax

To specify a BGP confederation identifier, use the bgp confederation identifier command. To remove the confederation identifier, use the no form of this command

bgp confederation identifier autonomous-system

no bgp confederation identifier autonomous-system

Parameter

parameter	description
autonomous-system	Autonomous system number to be configured to internally include multiple autonomous systems

Default value

none

Command mode

BGP configuration mode

Usage guidelines

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. In the Autonomous System Alliance, an AS that can be divided into several sub-ASs. Within each sub-AS, all IBGP rules apply, such as all IBGP neighbors must form a full mesh structure. Each sub-AS has a different AS number, so they EBGP must be run between sub-ASs. Although EBGP is used between sub-ASs, the routing performance within the confederation is similar to the IBGP routing within a single AS. That is, when crossing the boundaries of sub-ASs, Nexthop, MED, Localpreference information is preserved. To the others, the alliance looks like a single AS

An autonomous system alliance identifier is an autonomous system. All BGP switches in the same autonomous system alliance must be configured with the same autonomous system alliance identifier

Configuring the autonomous system alliance identifier often requires re-establishing BGP connections

Example

In the following example, the routing domain is divided into autonomous systems AS4001, 4002, 4003, 4004, 4005, 4006 and 4007 and identified by the confederation identifier 5. The local AS is 4001. Neighbor 1.2.3.4 is a peer inside of the routing domain confederation. Neighbor 3.4.5.6 is a peer outside of the routing domain confederation. For the neighbor 3.4.5.6, your AS is 5:

router bgp 4001

bgp confederation identifier 5

bgp confederation peers 4002 4003 4004 4005 4006 4007

neighbor 1.2.3.4 remote-as 4002

neighbor 3.4.5.6 remote-as 510

Related commands

bgp confederation peers

show ip bgp summary

62.11 bgp confederation peers

Syntax

To configure subautonomous systems to belong to a single confederation, use the bgp confederation peers command in router configuration mode. To remove an autonomous system from the confederation, use the no form of this command

bgp confederation peers autonomous-system [**autonomous-system**]

no bgp confederation peers [**autonomous-system**]

Parameter

parameter	description
autonomous-system	Autonomous system number

Default value

none

Command mode

BGP configuration mode

Usage guidelines

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. In the Autonomous System Alliance, an AS that can be divided into several sub-ASs. Within each sub-AS, all IBGP rules apply, such as all IBGP neighbors must form a full mesh structure. Each sub-AS has a different AS number, so they EBGP must be run between sub-ASs. Although EBGP is used between sub-ASs, the routing performance within the confederation is similar to the IBGP routing within a single AS. That is, when crossing the boundaries of sub-ASs, Nexthop, MED, Localpreference information is preserved. To the others, the alliance looks like a single AS

The autonomous system specified by this command is internal to the same autonomous system alliance and is a sub-autonomous system. Each sub-autonomous system is fully connected within itself

Generally, use the **bgp confederation identifier** command to specify which autonomous system alliance the local AS belongs to

Configuring this command often requires re-establishing BGP connections

Example

In the following example, autonomous systems 1091, 1092 and 1093 are configured to belong to a single confederation under the identifier 1090:

router bgp 1090

bgp confederation identifier 23

bgp confederation peers 1091 1092 1093

Related commands

bgp confederation identifier

show ip bgp summary

62.12 bgp dampening

Syntax

To enable BGP route dampening or change BGP route dampening parameters, use the **bgp dampening** command. To disable BGP dampening, use the no form of this command

bgp dampening [*half-time resuse-value suppress-value hold-time*]

no bgp dampening

Parameter

parameter	description
half-time	Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period.
reuse-value	Reuse values based on accumulated penalties
suppress-value	A route is suppressed when its penalty exceeds this limit
hold-time	Maximum time (in minutes) a route can be suppressed

Default value

half-time:15 minutes

reuse-value:750

suppress-value: 2000

hold-time:60 minutes

Command mode

BGP configuration mode

Usage guidelines

Route fluctuation control has different effects on routes in different states, mainly affecting whether the route is advertised to neighbors and whether it can be aggregated, and whether it is added to the main routing table. According to the fluctuation process of a route, its changes are described as follows:

A stable route is punished due to fluctuations. When its penalty value is less than the minimum penalty value of the suppressed route, it continues to advertise to neighbors and can be aggregated; when the penalty value of the route exceeds the Suppress value, it stops advertising to neighbors and stop being aggregated; when the route is stable, its penalty value can be reduced with time. It is always in a suppressed state until its penalty value reaches the maximum penalty value of the reused route (Reuse), and it cannot advertise to neighbors and be aggregated; When the penalty value drops below Reuse, the route becomes effective and can advertise to neighbors and be aggregated

Example

In the following example, the bgp dampening command can be used to enable BGP route dampening function and use default parameter configuration. Use the following commands to configure different dampening parameters for different rouing configurations:

Router bgp 100

bgp dampening

Related commands

None

62.13 bgp default local-preference

Syntax

To configure default parameter of BGP process, use the bgp default command. Use the no form of this command to restore the default value

bgp default local-preference *<0-4294967295>*

no bgp default local-preference

Parameter

parameter	description
local-preference	Configures default parameter of the local preference
<0-4294967295>	Default value of the local preference

Default value

100

Command mode

BGP configuration mode

Usage guidelines

The route received from IBGP will be set as the local preference by BGP. The default value is 100, which can be modified via this command

Example

The following example configures 200 as the local preference for the route from IBGP neighbor:

router bgp 100

bgp default local-preference 200

Related commands

None

62.14 bgp default route-target filter

Syntax

To set BGP VPN route filter function, run the following command. To return to the default setting, use the no form of this command

bgp default route-target filter

no bgp default route-target filter

Parameter

None

Default value

Enabled

Command mode

BGP configuration mode

Usage guidelines

The command is enabled by default. It is used to control VPN multi-communication. To disable the filter function, run the command "no bgp default route-target filter", which means all VPN routes are received, generally applied to the solution of cross-domain VPN option-B

Example

The following example shows how to enable all VPN routes passing

router bgp 100

no bgp default route-target filter

Related command

None

62.15 bgp deterministic-med

Syntax

To modify BGP's handling of MED attributes, use the following command. To restore the default values, use no form of the command

bgp deterministic-med

no bgp deterministic-med

Parameter

none

Default value

none

Command mode

BGP configuration mode

Usage guidelines

By default, comparison of the Multi Exit Discriminator (MED) for routes from different neighbors in the same autonomous systems is enabled. The **bgp bestpath med confed** command is used to enable the comparison of the Multi Exit Discriminator (MED) for routes from different neighbors in the same autonomous systems alliance. This command is to make BGP compare MED to routes from different neighbors with the same autonomous system and the same sub-autonomous system

Example

none

Related commands

bgp bestpath med

bgp always-compare-med

62.16 bgp fast-external-fallover

Syntax

To enable fast clear neighbor function, run the following command. To return to the default setting, use the no form of this command

bgp fast-external-fallover

no bgp fast-external-fallover

Parameter

None

Default value

Enabled

Command mode

BGP configuration mode

Usage guidelines

The function is enabled by default. If the interface status becomes **Down**, it will immediately clear the BGP dialogue of the direct external neighbor on the interface

Example

None

Related command

router bgp

clear ip bgp

62.17 bgp graceful-restart

Syntax

To configure bgp graceful restart, run the following command

bgp graceful-restart [**restart-time** value] | [**stalepath-time** value]

no bgp graceful-restart [restart-time] | [stalepath-time]

Parameter

Parameter	Description
restart-time	To configure the max waiting time of protocol restarting neighbor up. The default value is 120s
stalepath-time	To configure the max stalepath time of restarting the neighbor and aging the route. The default value is 360s

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

bgp graceful-restart restart-time

The command is used to configure Restart Time of BGP GR, which is used by Receiving Speaker

bgp graceful-restart stalepath-time

The configuration time should be the time of keeping aging route

Example

None

Related command

bgp update-delay

clear ip bgp

62.18 bgp maxas-limit

Syntax

To configure the max amount limit of as which bgp route passes, run the following command

bgp maxas-limit <value>

no bgp maxas-limit

Parameter

Parameter	Description
value	The value ranges from 1 to 500

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to limit the amount of **as** which is part of **aspath** of routes received by the neighbor. The value will de dropped if the amount of **as** is greater than the configured value

Example

None

Related command

clear ip bgp

62.19 bgp router-id

Syntax

To configure bgp router identifier, run the following command

bgp router-id *<A.B.C.D>*

no bgp router-id *<A.B.C.D>*

Parameter

Parameter	Description
A.B.C.D	To be configured ID

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to configure a new router ID. Peer in the state of Established will automatically resume to BGP

Example

None

Related command

clear ip bgp

show ip bgp

62.20 bgp update-delay

Syntax

To configure bgp route update delay, run the following command. To return to the default setting, use the no form of this command

bgp update-delay <value>

no bgp update-delay

Parameter

Parameter	Description
value	Time of the route update delay. The value ranges from 1 to 3600s

Default value

360s

Command mode

BGP configuration mode

Usage guidelines

The command takes effect only when BGP supports GR. After BGP restart, BGP will not send the firstly update packets to local RIB until the timer is overtime. The BGP process re-selects the optimal route and then advertises it. That is to say, after BGP restarts, BGP will wait until this timer expires before sending the first update message

Another condition is that BGP updates without waiting for overtime of the timer. Refer to the command "**bgp graceful restart**" for more information

Example

None

Related command

bgp graceful-restart

clear ip bgp

62.21 bgp redistribute-internal

Syntax

To configure IBGP redistribution into an interior gateway protocol (IGP), such as RIP or OSPF, use the **bgp redistribute-internal** command. To return the router to default behavior and stop iBGP redistribution into IGPs, use the no form of this command

bgp redistribute-internal

no bgp redistribute-internal

Parameter

none

Default value

IBGP routes are not redistributed into IGP

Command mode

BGP configuration mode

Usage guidelines

When configuring this command, you must pay attention to the configuration between the switches, otherwise it is easy to cause routing loops. After configuring this command, use the command **clear ip bgp *** to reset BGP

Example

In the following example, BGP to OSPF3 route redistribution is enabled:

router ospf 3

redistribute bgp 2

!

router bgp 2

bgp redistribute-internal

!

Related commands

None

62.22 clear ip bgp

Syntax

To reset Border Gateway Protocol (BGP) connections using soft reconfiguration, use the clear ip bgp command

clear ip bgp {***** | *ip-address* | ipv6-address | as-number |dampening | **peer-group** *name* | **aggregates** | **networks** | **redistribute}** [**soft** [**in** [prefix-filter]| **out**]]

Parameter

parameter	description
*	Specifies that all current BGP sessions will be reset
ip-address	Specifies that only the identified BGP neighbor will be reset
ipv6-address	Reset the specified IPv6 address neighbor
as-number	Specifies that sessions with BGP peers in the specified autonomous system will be reset
dampening	Clear routing information suppressed by fluctuations
peer-group name	Specifies that the identified BGP peer group will be reset
aggregates	Specifies that all aggregate routes will be reset
networks	Specifies that all static network routes will be reset
redistribute	Specifies that all redistributed routes will be reset
soft	Initiates a soft reset
in | out	Initiates inbound or outbound reconfiguration
prefix-filter	Soft reconfiguration of ORF inbound routin

Command mode

EXEC

Usage guidelines

Some BGP policy configurations will not take effect immediately, because the route will only be sent once in a BGP session, so you need to reset the BGP session to send the routing information again

If the BGP soft reconfiguration is specified by command with the **soft** keyword, the session will not be reset, and the switch sends all the routing update information again. To generate new inbound update information

without resetting the BGP session, local BGP session participants should use **neighbor soft-reconfiguration** command to stores all updates received without modification, regardless of whether it is received by the inbound policy. Because this process has a large amount of storage, it should be avoided as much as possible. Outbound BGP soft configuration does not require any additional memory overhead. You can trigger an outbound reconfiguration at the other end of the BGP session to make the new inbound policy take effect

When using **aggregates, networks, and redistribute,** the **soft** option cannot be used. They will clear the specified type of route and regenerate a new one to make the new configuration take effect

Example

The following example reset all the current BGP sessions:

clear ip bgp *

Related commands

neighbor soft-reconfiguration

show ip bgp

62.23 debug ip bgp

Syntax

To display information related to processing of the Border Gateway Protocol (BGP), use the **debug ip bgp** command. To disable debugging output, use the no form of this command

debug ip bgp {all | dampening | event | fsm | keepalive | notify | open | vrf | update }

no debug ip bgp {all | dampening | event | fsm | keepalive | notify | open | vrf | update }

Parameter

parameter	description
all	Displays all BGP debugging functions
dampening	Displays BGP dampening
event	Displays BGP events
fsm	Displays BGP fsms
keepalive	Displays BGP keepalives
notify	Displays BGP notifies
open	Displays BGP opens
vrf	Enable BGP vrf configuration information tracking
update	Displays BGP updates

Default value

All tracking functions are disabled

Command mode

EXEC

Usage guidelines

It is valid globally when configured with the **debug ip bgp** command to display debugging information. If other VTY are configured with the terminal monitor command, the debugging information will also be displayed. Use the **no terminal monitor** to close this function to disable displaying any debugging information on the VTY

The command **debug ip bgp all** can enable all BGP debugging function, including dampening, fsm,keepalives,open and update. Use the **no debug ip bgp all** command to disable all BGP debugging functions

Example

The following example is the process to establish a BGP. The debugging information shows that a switch establishes a connection with BGP neighbor 10.1.1.3. The status changes from Idle to Established, indicating that the connection is established. Various packets information includes receiving Open, sending Open message, sending Keepalive, receiving Keepalive, etc

The format of the debugging information includes several main parts. The first may be time information, which depends on whether the configuration allows time information to be adde. The information that really belongs to BGP is behind the time information: first indicates the information is about the BGP header information "BGP:", then the specific BGP neighbor address, and then the specific BGP event information

BGP: 10.1.1.3 start connecting to peer

BGP: 10.1.1.3 went from Idle to Connect

BGP: 10.1.1.3 went from Connect to OpenSent

BGP: 10.1.1.3 send OPEN, length 41

BGP: 10.1.1.3 recv OPEN, length 41

BGP: 10.1.1.3 went from OpenSent to OpenConfirm

BGP: 10.1.1.3 send KEEPALIVE, length 19

BGP: 10.1.1.3 recv KEEPALIVE, length 19

BGP: 10.1.1.3 went from OpenConfirm to Established

BGP: 10.1.1.3 send KEEPALIVE, length 19

BGP: 10.1.1.3 send UPDATE, length 43

BGP: 10.1.1.3 send UPDATE, length 43

BGP: 10.1.1.3 recv KEEPALIVE, length 19

BGP: 10.1.1.3 recv KEEPALIVE, length 19

62.24 distance

Syntax

To configure the administrative distance for BGP routes, use the **distance** command. To return to the administrative distance to the default value, use the no form of this command

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Parameter

parameter	description
external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The default value is 20
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The default value is 200
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The default value is 200

Default value

external-distance: 20

internal-distance: 200

local-distance: 200

Command mode

BGP configuration

Usage guidelines

The **distance** command is used to modify the management distance of the route, the priority of the route, and the route selection, to achieve the routing management strategy

Changing the managemen distance of a route is dangerous unless you know exactly what you are doing. This action may increase the inconsistency of the routing table, which may damage the routing

Example

In the following example, the administrative distance for BGP routes is set:

router bgp 109

network 131.108.0.0

neighbor 129.140.6.6 remote-as 123

neighbor 128.125.1.1 remote-as 47

distance 20 20 200

Related commands

set metric

set tag

62.25 filter

Syntax

To filter routes based on an interface in order to realize the administrative strategy. Use the no form of this command to delete the configuration

filter interface <**in** | **out**> { **access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name* }

no filter interface <**in** | **out**> { **access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*

Parameter

parameter	description
interface	Interface name. Asterisk signifies all interfaces
in | **out**	Filter the incoming of outgoing routes
access-list	Specifies the access-list to filter routes
access-list-name	Name of the access list
gateway	Specifies the access list to filter gateway
access-list-name	Name of the access list
prefix-list	Specifies the prefix list to filter routes
prefix-list-name	Name of the prefix list

Default value

none

Command mode

BGP configuration mode

Usage guidelines

The **access-list** option specifies the access list to filter network prefix of routes; the **gateway** option specifies the access list to filter nexthop attribute of routes; the **prefix list** option specifies the prefix list filter network prefix of routes

The **access list** and the **prefix list** options are mutually exclusive simultaneously. But then can be used with the **gateway** option together

The asterisk(*) signifies all interfaces. If the filtering rules are configured on the specific interface and all

interfaces, the route must meet all the filtering rules

If a none-existant **prefix list** or **access list** is configured on an interface, then all routes will pass

Example

The following example configures prefix-list and gateway to filter routes received on all interface:

router bgp 109

filter * in prefix-list prefix-guize gateway gateway-guize

Related commands

neighbor distribute-list

neighbor filter-list

neighbor route-map

62.26 maximum-paths

Syntax

To enable bgp supporting equivalent route, run the **maximum-paths** command. To return to the default setting, use the no form of this command

maximum-paths [*value*] [**ibgp** value]

no maximum-paths [*value* | **ibgp**]

Parameter

Parameter	Description
value	Max amount of the equivalent route supported by BGP

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to modify the amount of bgp supported equivalent routes. Parameters without ibgp is the modified amount of the EBGP equivalent route, which will not affect the choosing result of the optimized routes

Example

The following example shows how to set the equivalent route which supports 3 ibgp:

router bgp 100

maximum-paths ibgp 3

Related command

clear ip bgp

show ip bgp

62.27 neighbor activate

Syntax

To activate the specified neighbor corresponded address family routing information, run the **neighbor** command. To return to the default setting, use the no form of this command

neighbor {*ip-address*| *X:X::X:X* | *peer-group-name*} **activate**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **activate**

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	Ipv6 address of the neighbor
peer-group-name	Peer group name

Default value

Activated

Command mode

BGP address protocol stack configuration mode

Usage guidelines

The command is used to activate the support for the specified neighbor corresponded address family routing information

Example

None

Related command

neighbor remote-as

62.28 neighbor advertisement-interval

Syntax

To set the minimum interval of forwarding UPDATE information, run the following command. To return to the default setting, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **advertisement-interval** *value*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **advertisement-interval**

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	Ipv6 address of the neighbor
peer-group-name	BGP peer group name
Value	<1-600> Unit: s

Default value

ibgp: The default value is 1s

ebgp: The default value is 30s

Command mode

BGP configuration mode

Usage guidelines

The command is used to set the minimum interval of forwarding UPDATE information

Example

The following example shows how to set the minimum interval of the neighbor 10.10.10.11 forwarding UPDATE information to 15s

router bgp 1

neighbor 10.10.10.11 remote-as 2

neighbor 10.10.10.11 advertisement-interval 15

Related command

neighbor remote-as

62.29 neighbor allowas-in

Syntax

To enable BGP receiving route which including **as** from the neighbor learned **aspath**, run the following command. To disallow receiving similar routes, use no form of the command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **allowas-in** [*value*]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **allowas-in**

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
Value	<1-10> Times which enable locak as appeared in the attribute of aspath. The default value is 3

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

The command is used to enable BGP receiving route which including **as** from the neighbor learned **aspath**

Example

The following example shows how to enable BGP receiving route which including as (3 times in maximum) from the neighbor (10.10.10.11) learned aspath:

router bgp 1

neighbor 10.10.10.11 remote-as 2

neighbor 10.10.10.11 allowas-in

Related command

neighbor remote-as

62.30 neighbor capability orf prefix-list

Syntax

To enable ORF, run the following command. To return to the default setting, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **capability orf prefix-list** {both| receive| send}

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **capability orf prefix-list** {both| receive| send}

Parameter

Parameter	Description

ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name

Default value

Non-support

Command mode

BGP configuration mode

Usage guidelines

The command enables BGP to support ORF. ORF is a filtration mode based on prefix-list. It only informs the local required routes to the neighbor, reducing the unnecessary update packets. The command is used by combining with the command "neighbor prefix-list in". The command takes effect only when combining with the command "clear ip bgp *"

Example

The following example shows how to set the output route filtration of neighbor 10.10.10.11(receiving and forwarding):

router bgp 100

neighbor 10.10.10.11 remote-as 2

neighbor 10.10.10.11 capability orf prefix-list both

Related command

neighbor prefix-list in

clear ip bgp in prefix-filter

62.31 neighbor default-originate

Syntax

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the neighbor default-originate command. To send no route as a default, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **default-originate** [route-map *map-name*]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **default-originate**

Parameter

parameter	description
ip-address	IP address of the neighbor

X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
route-map	Set routing attributes with route-map
map-name	Name of route-map

Default value

No default route is sent to the neighbor

Command mode

BGP configuration mode

Usage guidelines

Configure this command to send the default route to the neighbor immediately

This command has nothing to do with whether route 0.0.0.0 is generated in the BGP routing table

Example

In the following example, The default route will be advertised to the neighbor 160.89.2.3 rather than to 160.89.2.1:

router bgp 109

network 160.89.0.0

neighbor 160.89.2.1 remote-as 100

neighbor 160.89.2.3 remote-as 200

neighbor 160.89.2.3 default-originate

Related commands

neighbor ebgp-multihop

62.32 neighbor description

Syntax

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode. To remove the description, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **description LINE**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **description**

Parameter

parameter	description

ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
line	Text that describes the neighbor

Default value

There is no description of the neighbor

Command mode

BGP configuration mode

Usage guidelines

It is easier for user to understand the configuration to associate a description with a neighbor

Example

In the following example, the description of the neighbor is "peer with abc.com":

router bgp 109

network 160.89.0.0

neighbor 160.89.2.3 description peer with abc.com

62.33 neighbor distribute-list

Syntax

Use the **neighbor distribute-list** command to configure the access list to filter the inbound and outbound routes of BGP neighbors. Use no form of the command to delete the configuration:

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

Parameter

parameter	description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
access-list name	Name of a standard or extended access list
In	Access list is applied to incoming advertisements to that neighbor

Out	Access list is applied to outgoing advertisements to that neighbor

Default value

none

Command mode

BGP configuration mode

Usage guidelines

One of the methods for neighbor-based filtering BGP route advertisements is to use **neighbor distribute-list**, which uses **access-list** to filter the network prefix information of BGP routes; one method is to use **neighbor filter-list**, which uses aspath-list to filter AS_PATH attribute; another method uses **neighbor prefix-list**, which uses prefix-list to filter the network prefix information

If you specify a non-existant access list, all routes will be allowed to pass as a result

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group

Example

The following router configuration mode example applies list beijing to incoming advertisements from neighbor120.23.4.1.

router bgp 109

network 131.108.0.0

neighbor 120.23.4.1 distribute-list beijing in

Related commands

ip aspath-list

neighbor filter-list

ip prefix-list 1

neighbor prefix-list

62.34 neighbor ebgp-multihop

Syntax

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ebgp-multihop** *ttl*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ebgp-multihop**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor
X:X::X:X	BGP session neighbor IPv6 address
peer-group-name	BGP peer group name
ttl	Time-to-live in the range from 1 to 255 hops

Default value

For EBGP-speaking neighbor, only directly connected neighbors are allowed, ttl default value is 1; for IBGP-speaking neighbor, ttl default is 255

Command mode

BGP configuration mode

Usage guidelines

By default, BGP connection can not be established unless EBGP neighbors are directly connected ones. The allowable maximum number of hops for EBGP neighbors can be set with the **neighbor ebgp-multihop** command

Ttl is configured to 255 if not specified

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command

Example

The following example allows connections to neighbor 131.108.1.1, which resides on a network that is not directly connected:

router bgp 109:

neighbor 131.108.1.1 ebgp-multihop

Related commands

neighbor default-originate

62.35 neighbor fall-over

Syntax

To activate bfd link detection function of the neighbor, run the following command. To return to the default setting, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **fall-over bfd**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **fall-over bfd**

Parameter

Parameter	Description
ip-address	BGP dialogue neighbor IP address
X:X::X:X	BGP dialogue neighbor IPv6 address
peer-group-name	BGP peer group name

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

The command is used to detect the link. If there is problem in the link, bfd will inform bgp to update the route, which will realize fast switch of the route

Example

none

Related command

neighbor remote-as

bfd enable

62.36 neighbor filter-list

Syntax

To configure the as-path list to filter the inbound and outbound routes of BGP neighbors, use the neighbor filter-list command. To disable this function, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

no neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

Parameter

parameter	description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
as-path-list name	AS-PATH list name. The ip as-path-list command can be used to define this list

In	Access list applied to incoming routes
Out	Access list applied to outgoing routes

Default value

none

Command mode

BGP configuration mode

Usage guidelines

One of the methods for neighbor-based filtering BGP route advertisements is to use **neighbor distribute-list**, which uses **access-list** to filter the network prefix information of BGP routes; one method is to use **neighbor filter-list**, which uses aspath-list to filter AS_PATH attribute; another method uses **neighbor prefix-list**, which uses prefix-list to filter the network prefix information

If you specify a non-existant aspath-list, all routes will be allowed to pass as a result

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group

Example

In the following example, the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system AS123:

ip as-path-list shanghai deny _123_

ip as-path-list shanghai deny ^123$

router bgp 109

network 131.108.0.0

neighbor 129.140.6.6 remote-as 123

neighbor 128.125.1.1 remote-as 47

neighbor 128.125.1.1 filter-list shanghai out

Related commands

ip aspath-list

neighbor distribute-list

ip prefix-list1

neighbor prefix-list

62.37 neighbor maximum-prefix

Syntax

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. To disable this function, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **maximum-prefix** *maximum* [**warnning-only**]

no neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **maximum-prefix**

Parameter

parameter	description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
Maximum	Maximum number of prefixes allowed from this neighbor
warnning-only	Only give warning message when the route exceeds the limit.

Default value

This command is disabled by default. There is no limit on the number of prefixes

Command mode

BGP configuration mode

Usage guidelines

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer. When the number of received prefixes exceeds the maximum number configured, the router terminates the peering

Example

The following example sets the maximum number of prefixes allowed from the neighbor at 129.140.6.6 to 1000:

router bgp 109

network 131.108.0.0

neighbor 129.140.6.6 maximum-prefix 1000

Related commands

clear ip bgp

62.38 neighbor next-hop-self

Syntax

To activate the next-hop processing of BGP updates in the switch and set itself as the next-hop address, use

the **neighbor next-hop-self** command. To disable this feature, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **next-hop-self**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **next-hop-self**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor
X:X::X:X	BGP session IPv6 address of the neighbor
peer-group-name	BGP peer group name

Default value

This command is disabled by default

Command mode

BGP configuration mode

Usage guidelines

The disposal of nexthop attribute in BGP is more complicated than IGP. It usually follows three rules:

For EBGP session, configure the local ip address of BGP connection as the nexthop attribute when sending routes

For IBGP session, configure the local ip address of BGP connection as the nexthop attribute if the routes are locally generated; if the routes are learned from EBGP, the nexthop attribute is to be filled in intactly the packet when sending routes

If the nexthop parameter of the ip address of the routes belong to the network of BGP session, then the nexthop attribute always adopts the former nexthop

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group

Example

The following example forces all updates destined for 131.108.1.1 to advertise this router as the next hop:

router bgp 109

neighbor 131.108.1.1 next-hop-self

Related commands

set ip next-hop18

62.39 neighbor password

Syntax

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** command. To disable this function, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **password** *[type] LINE*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **password**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
password	Enables MD5 authentication
type	Password encapsulation type: 0, 6, 7 0 means that the configuration and display are in plain text; 6 indicates that the configuration is in plain text and displayed in cipher text; 7 indicates that the configuration and display are in cipher text Note: The case of not configuring the type is considered as type 0
LINE	Plainr text password

Default value

none

Command mode

BGP configuration mode

Usage guidelines

Use the neighbor remote-as command to specify the neighbor before using this command

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The length of password should between 1 and 100 characters(type 7 is 202)

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command

Example

The following example configures 'abcd' as the authentication password of neighbor 120.23.4.1:

router bgp 109

neighbor 120.23.4.1 remote-as 108

neighbor 120.23.4.1 password abcd

Related commands

neighbor remote-as

62.40 neighbor peer-group

Use the **neighbor peer-group-name peer-group** command to configure the peer group. Use **no neighbor peer-group-name peer-group** to delete the configured peer group

Use the **neighbor ip-address peer-group-name** command to configure the neighbor to join the peer group. Use the **no neighbor ip-address peer-group peer-group-name** to delete the neighbor added to the peer group

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

neighbor {*ip-address* | *X:X::X:X*} **peer-group** *peer-group-name*

no neighbor {*ip-address* | *X:X::X:X*} **peer-group** *peer-group-name*

Parameter

Parameter	Description
ip-address	Neighbor IP address
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name

Default

None

Command mode

BGP configuration mode

Usage guidelines

Use the **neighbor peer-group-name peer-group** command to configure the peer group

Use the **neighbor ip-address peer-group-name** command to configure the neighbor to join the peer group. If there is no configuration on previous neighbor, use this command to configure the peer group's autonomous system number first

Example

The following example configures a peer group named group, and then configures neighbor 10.1.1.1 to join the peer group:

router bgp 1

neighbor group peer-group

neighbor group remote-as 2

neighbor 10.1.1.1 peer-group group

Related command

neighbor remote-as

62.41 neighbor prefix-list

Syntax

To configure prefix-list to filter neighbor routing updates, use the **neighbor prefix-list** command. To remove a filter list, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

Parameter

parameter	description
ip-address	IP address of neighbor
X:X::X:X	Neighbor IPv6 address
peer-group-name	BGP peer group name
prefix-list	Prefix list is applied to advertisements of that neighbor
prefix-listname	Name of a prefix list
In	Filter list is applied to incoming advertisements from that neighbor
Out	Filter list is applied to outgoing advertisements to that neighbor

Default value

none

Command mode

BGP configuration mode

Usage guidelines

One of the methods for neighbor-based filtering BGP route advertisements is to use **neighbor distribute-list**, which uses **access-list** to filter the network prefix information of BGP routes; one method is to use **neighbor filter-list**, which uses aspath-list to filter AS_PATH attribute; another method uses **neighbor prefix-list**, which uses prefix-list to filter the network prefix information

If you specify a non-existant prefix-list, all routes will be allowed to pass as a result

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group

Example

The following router configuration mode example applies the prefix list named abc to incoming advertisements from neighbor 120.23.4.1:

router bgp 109

network 131.108.0.0

neighbor 120.23.4.1 prefix-list abc in

The following router configuration mode example applies the prefix list CustomerA to incoming advertisements from neighbor 120.23.4.1:

router bgp 109

network 131.108.0.0

neighbor 120.23.4.1 prefix-list CustomerA in

Related commands

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

neighbor filter-list

62.42 neighbor remote-as

Syntax

To create a BGP neighbor and specify its autonomous system number, use the neighbor remote-as command in router configuration mode. To the neighbor and all its configurations, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remote-as** *number* [passive]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remote-as** *number*

Parameter

parameter	description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor

peer-group-name	BGP peer group name
Number	Nmuber of autonomous system to which the neighbor belongs
passive	This parameter indicates that the neighbor is configured in passive mode, and will not initiate a TCP connection actively

Default value

none

Command mode

BGP configuration mode

Usage guidelines

The neighbor with the same AS number specified in the **router bgp** command is considered to be IBGP. Otherwise, the neighbor is considered to be EBGP. This command is used to create a neighbor. Only after the neighbor is created, other commands about the neighbor can be configured. If the neighbor has been configurated, you can change its autonomous system number, which will cause the BGP connection to reset

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command

Example

In the following example, the local autonomous system is 109, the autonomous systems of neighbors 131.108.200.1, 131.108.234.2, 150.136.64.19 are configured as 167, 109, 99.

router bgp 109

network 131.108.0.0

network 192.31.7.0

neighbor 131.108.200.1 remote-as 167

neighbor 131.108.234.2 remote-as 109

neighbor 150.136.64.19 remote-as 99

Related commands

neighbor peer-group (creating)

62.43 neighbor remove-private-AS

Syntax

To remove private aspath when informing the route to ebgp neighbor, run the following command. To return to the default setting, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remove-private-AS**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remove-private-AS**

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name

Default value

None

Command mode

BGP configuration mode

Usage guidelines

None

Example

In the following example, the local autonomous system is 100, the neighbor is 10.1.1.1, 20.1.1.1, the autonomous system is 64512, 200. The command is used to delete private aspath attribute when informing 10.1.1.1 learned route to ebgp neighbor 20.1.1.1.

router bgp 100

neighbor 10.1.1.1 remote-as 64512

neighbor 20.1.1.1 remote-as 200

neighbor 20.1.1.1 remove-private-AS

Related command

neighbor remote-as

62.44 neighbor route-map

Syntax

To apply a ROUTE-MAP to filter the neighbor's inbound and outbound routes, or modify its attributes, use the **neighbor route-map** command. To remove a route map, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}

no neighbor {*ip-address* |*X:X::X:X* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}

Parameter

parameter	description

ip-address	IP address of the neighbor
X:X::X:X	The neighbor's IPv6 address
peer-group-name	Name of a BGP or multiprotocol BGP peer group
map-name	Name of a route map
in	Applies route map to incoming routes
Out	Applies route map to outgoing routes

Default value

none

Command mode

BGP configuration mode

Usage guidelines

It is only based on neighbor to filter routes using distribute-list, prefix-list and as-path-list, while with route-map, it is not only based on neighbor to filter routes but also based on neighbor to modify the attribute of routes to realize a more flexible routing strategy

Different routes have different attributes. The route-map can modify attributes of different kinds of routes. If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map. The rules which is valid to BGP route are as follows: match aspath-list, match community-list, match ip address, match ip nexthop, match ip prefix-list, match metric, match tag, set aggregator, set as-path, set atomic-aggregate, set community, set community-additive, set ip nexthop, set local-preference, set metric, set origin, set tag, set weight

If configured with a non-existent route-map, then all routes is allowed to receive as a result without any modification

If you specify a BGP or multiprotocol BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group

Example

The following example applies a route map named internal-map to a BGP incoming route from 198.92.70.24:

router bgp 5

neighbor 198.92.70.24 route-map internal-map in

route-map internal-map

match as-path abc

set local-preference 100

Related commands

neighbor peer-group (creating)

route-map

62.45 neighbor route-reflector-client

Syntax

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command. To indicate that the neighbor is not a client, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **route-reflector-client**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* }| **route-reflector-client**

Parameter

parameter	description
ip-address	IP address of the BGP neighbor being identified as a client
X:X::X:X	The neighbor's IPv6 address
peer-group-name	BGP peer group name

Default value

There is no route reflector in the autonomous system

Command mode

BGP configuration mode

Usage guidelines

By default, all internal BGP (iBGP) sessions in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop

If you use route reflectors, all iBGP sessions need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector

Example

In the following example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 198.92.70.24.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
```

Related commands

bgp cluster-id

show ip bgp

62.46 neighbor route-refresh

Syntax

To allow neighbor to use route refresh function, use the neighbor route-refresh command. Use the no form of this command to disable route refresh function

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **route-refresh**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **route-refresh**

Parameter

parameter	description
ip-address	BGP neighbor and ip address
X:X::X:X	The neighbor's IPv6 address
peer-group-name	BGP peer group name

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

By default, BGP route exchange for only once when the connection is established, then only exchanging changed routes afterwards. If the routing strategy configuration is modified, it will not become effective immediately. Generally, there are two methods:

- Reset BGP connection
- Use soft-reconfiguration function

The first method is relatively slow, and the routes vary greatly. The second method needs too much storage space and occupies more CPU time. These two methods are not good method, and therefore a new method arises, that is, the route refresh

The route refresh is a negotiation option based on BGP connection, aiming to send the route refresh request packet to ask neighbor to re-send all update packets to oneself, which do not need to reset BGP connection and also do not need to store a great amount of routes. This a a more ideal solution at the moment

Example

The following example allows neighbor at address 198.92.70.24 to use route refresh function:

router bgp 5

neighbor 198.92.70.24 route-refresh

Related commands

show ip bgp neighbors

62.47 neighbor send-community

Syntax

To specify that a community attribute should be sent to a BGP neighbor, use the neighbor send-community command. To remove the entry, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **send-community** [**standard** | **extended** | **both**]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* }**send-community** [**standard** | **extended** | **both**]

Parameter

parameter	description
ip-address	IP address of the neighbor
X:X::X:X	The neighbor's IPv6 address
peer-group-name	BGP peer group name

Default value

The communities attribute can be sent to the neighbor

Command mode

BGP configuration mode

Usage guidelines

By default, community attributes are not allowed to be sent to neighbors. **Neighbor send-community** command can be used to send routes with community attributes to neighbors

Use the **show ip bgp neighbors** command to see whether allows to send group attribute to neigh or not

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command

Example

In the following example, the switch belongs to autonomous system 109 and is configured to send the COMMUNITIES and EXTCOMMUNITIES attributes to the neighbor at IP address 198.92.70.23:

router bgp 109

no neighbor 198.92.70.23 send-community both

Related commands

match community-list4

set community15

set community-additive17

62.48 neighbor send-label

Syntax

To activate neighbor or peer group NLRI with tag, run the following command. To return to the default setting, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **send-label**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* }**send-label**

Parameter

Parameter	Description
ip-address	IP address of neighbor
X:X::X:X	IPv6 address of neighbor
peer-group-name	BGP peer group name

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to activate **nlri** with **mpls** tag, which is usually applied in cross-domain vpn option solution. The command must be combined with command "route-map", if mpls tag is distributed by the public network

Related command

neighbor remote-as

neighbor route-map

show ip bgp neighbors

62.49 neighbor shutdown

Syntax

To disable a neighbor or peer group, use the **neighbor shutdown** command in router configuration mode. To reenable the neighbor or peer group, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **shutdown**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* }**shutdown**

Parameter

parameter	description
ip-address	IP address of the neighbor
X:X::X:X	The neighbor's IPv6 address
peer-group-name	BGP peer group name

Default value

none

Command mode

BGP configuration mode

Usage guidelines

The **neighbor shutdown** command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly

To display a summary of BGP neighbors and peer group connections, use the **show ip bgp summary** or **show ip bgp neighbors** command. Those neighbors with an Idle status and the Admin entry have been disabled by the **neighbor shutdown** command

Related commands

show ip bgp summary

show ip bgp neighbors

62.50 neighbor soft-reconfiguration

Syntax

To configure the software to start storing updates, use the neighbor soft-reconfiguration command in router configuration mode. To not store received updates, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **soft-reconfiguration inbound**

no neighbor {*ip-address*|*X:X::X:X*|*peer-group-name*} **soft-reconfiguration inbound**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor

X:X::X:X	The neighbor's IPv6 address
peer-group-name	BGP peer group name
inbound	Indicates that the update to be stored is an incoming update

Default value

The incoming update is not stored and the outgoing update is stored

Command mode

BGP configuration mode

Usage guidelines

Outbound routing updates will always be stored, and inbound routing updates will only be stored after they are configured. Storing routing updates can take effect without changing the BGP session after changing the routing policy. Resetting the BGP session will bring a lot of network data exchange, and it causes a lot of routing fluctuations. Using soft reconfiguration can avoid a lot of network data exchange and minimize routing fluctuations

Outbound routing updates are always stored. Inbound routing updates are not stored by default. After changing the local configuration policy, there are three ways to make the new configuration take effect:

First, reset the related BGP session; second, perform local inbound routing soft reconfiguration **clear ip bgp a.b.c.d soft in** (the local switch must be configured with neighbor a.b.c.d soft-reconfiguration); third, the other party performs outbound routing update soft reconfiguration **clear ip bgp a.b.c.d soft out** (no additional configuration required)

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command

Example

The following example enables inbound soft reconfiguration for the neighbor 131.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy

router bgp 100

neighbor 131.108.1.1 remote-as 200

neighbor 131.108.1.1 soft-reconfiguration inbound

Related commands

clear ip bgp

neighbor peer-group (creating)

62.51 neighbor timers

Syntax

To set the timers for a specific BGP peer or peer group, use the neighbor timers command in router configuration mode. To clear the timers for a specific BGP peer or peer group, use the no form of this command

neighbor {*ip-address|X:X::X:X|peer-group-name*} **timers** keepalive *holdtime* [*ldleholdtime*]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **timers**

Parameter

parameter	description
ip-address	A BGP peer or peer group IP address
X:X::X:X	The neighbor's IPv6 address
peer-group-name	Name of the BGP peer group
Keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer
Holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead. The range is: 0 or greater than 3
Idleholdtime	The Idleholdtime timer value in seconds

Default value

keepalive: 30 s

holdtime: 90 s

Idleholdtime: 0

Command mode

BGP configuration mode

Usage guidelines

The timer configured for a specific neighbor or peer group overrides the default BGP neighbor timer. Generally, the holdtime is 3 times that of keepalive. If keepalive and holdtime are set to 0, sending keepalive packets is prohibited. At this time, the tcp connection manager need to notify the BGP module that the state of the connection has changed

Idleholdtime is not 0, which means that the DampPeerOscillation function is activated. When the bgp peer is connected/disconnected 10 times within 5mins, the idleholdtimer is suppressed to keep the bgp peer in the idle state, and the keeping time is the configured idleholdtime

When Idleholdtime is 0, the DampPeerOscillation function is disabled

Example

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.98.47.10:

router bgp 109

neighbor 192.98.47.10 timers 70 210

62.52 neighbor ttl-security-hop

To configure TTL hop limit for BGP, run the following command. To return to the default setting, use the no

form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ttl-security-hop** *value*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ttl-security-hop**

Parameter

Parameter	Description
ip-address	IP address of neighbor
X:X::X:X	IPv6 address of neighbor
peer-group-name	peer group name of BGP
value	Value of hop limit. The value ranges from 1 to 254

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to configure the max hop supported by bgp neighbor. The connection exceeds this hop cannot be established

Example

The following example shows how to configure neighbor 10.1.1.2 ttl hop limit to 1:

router bgp 100

neighbor 10.1.1.2 ttl-security-hop 1

Related command

neighbor peer-group (creating)

neighbor remote-as

62.53 neighbor update-source

To have the software allow Border Gateway Protocol (BGP) sessions to use specified interface for TCP connections, use the **neighbor update-source interface** command. To restore the automatically selected interface, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **update-source interface**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **update-source**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor
X:X::X:X	The neighbor's IPv6 address
peer-group-name	BGP peer group name
Interface	Interface name

default

Use the local port IP address calculated from the route to establish a TCP connection

Command mode

BGP configuration mode

Usage guidelines

By default, the ip module decides the local ip address of TCP connection when BGP establishes the connection. IP module decides interface depending on routes, and then binds the main ip address of this interface as the local address of TCP. Use the update-source command can bind the main ip address of the local specified interface during the establishment of TCP connection

It is generally specified to use loopback interface, for the loopback interface 's protocol state is always up. And so this keeps the stability of BGP session and avoids route fluctuation

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command

Example

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface:

router bgp 110

network 160.89.0.0

neighbor 160.89.2.3 remote-as 110

neighbor 160.89.2.3 update-source Loopback0

Related commands

neighbor peer-group (creating)

62.54 neighbor weight

Syntax

To assign a weight to a neighbor connection, use the **neighbor weight** command. To remove a weight assignment, use the no form of this command

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **weight** *weight*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **weight**

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	BGP peer group name
Weight	Weight to assign. Acceptable values are from 0 to 65535

Default value

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local switch have a default weight of 32768

Command mode

BGP configuration mode

Usage guidelines

BGP routing metric is the important standard to choose routes. The default metric of all routes that learned from neighbors is 0. Use **route-map** command to set metric for routes that learned from neighbor

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command

Example

The following router configuration mode example sets the weight of all routes learned via 151.23.12.1 to 50:

router bgp 109

neighbor 151.23.12.1 weight 50

Related commands

neighbor peer-group (creating)

set weight23

62.55 network (BGP)

Syntax

To specify the networks to be advertised by the Border Gateway Protocol (BGP), use the network command. To remove an entry from the routing table, use the no form of this command

network A.B.C.D/n [**route-map** *map-name* | **backdoor**]

no network A.B.C.D/n

Parameter

parameter	description
A.B.C.D/n	Network prefix that BGP will advertise
route-map	The specified route map
map-name	Name of the route map
backdoor	Backdoor network

Default value

No networks are specified

Command mode

BGP configuration mode

Usage guidelines

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table

A totally same route in the main routing table of IP is the basis for the network configured with the network command to become effective

A more precise or totally same route in the local BTP routing table is the basis for the network to become effective that configured with the **aggretgate-address** command

The length of mask code is generated in term of standard network type if not specified

Use the route-map to configure route's attribute

The backdoor network is used to modify route distance rather than to generate routes. It changes route's default distance that learned from the neighbor to the local route's distance. The default value is 200

The maximum number of network commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM

Example

The following example sets up network 131.108.0.0/8 to be included in the BGP updates:

router bgp 120

network 131.108.0.0/8

Related commands

redistribute (BGP)

aggregate-address

62.56 redistribute(BGP)

Syntax

To redistribute a route process to Border Gateway Protocol (BGP), use the redistribute command. To remove the redistribute command from the configuration file, use the no form of this command

redistribute protocol *process-id*[**route-map** *map-name*] [**metric** *value*]

no redistribute protocol *process-id*

Parameter

parameter	description
protocol	Type of routing protocol
process-id	Process id of routing protocol, such as process if of ospf
route-map	Applies route map to configure route attribute
map-name	Name of route map
metric	Redistribution routing Mertic
value	Metric value. The range is from 0 to 4294967295

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other

peers but not to be included by local IP routing table

Use redistribute command to include routes dynamically to BGP. The change of route source will be reflected to BGP automatically. The automatically-included routes will be informed to other neighbors. The configuration of the redistribute command will re-check the specified type of routes in the routing table. The outer routes in OSPF will not be included to BGP

Use the **route-map** to configure route's attribute

Example

The following example configures routes from OSPF process 23 to be redistributed into BGP:

router bgp 109

redistribute ospf 23

related commands

route-map1

62.57 router bgp

Syntax

To enable the BGP routing process or enter in BGP configuration mode, use the router bgp command in global configuration mode. To disable a routing process, use the no form of this command

router bgp *as-number*

no router bgp *as-number*

Parameter

parameter	description
as-number	Number of autonomous system

Default value

No BGP routing process is enabled by default

Command mode

Global configuration mode

Usage guidelines

The system allows to configure one BGP process at most. The BGP task is established in the process of system initialization, and it is activated when the BGP process is started up. The BGP task only receives information from command module without configuring the BGP process. It is not related to routing module or any other module and will not response other information. The related show and clear command are all invalid

Use no router bgp command to delete BGP process, and at the same time other configuration related to BGP will also be deleted, such as neighbors and so on. The BGP route in routing table is also be deleted

To configure BGP process using the **show running** and **show ip bgp summary** commands to check

Example

The following example configures a BGP process for autonomous system 200:

router bgp 200

Related commands

neighbor remote-as

62.58 show ip bgp

Syntax

To display entries in the Border Gateway Protocol (BGP) routing table, use the show ip bgp command in user EXEC or privileged EXEC mode

show ip bgp [**network**]

Parameter

parameter	description
network	Displays the specified routing information

Command mode

EXEC

Usage guidelines

The **show ip bgp** command is used to display the entire IPv4 BGP routing table. After specifying a network, only the detailed information of the network is displayed

Example

The following is a group of BGP displaying information. The former two lines display some marked information

Status code indicates the status of the table entry. The status is displayed at the beginning of each line in the table. S indicates the table entry is suppressed, which is the invalid route and will not be chosen. D indicates the table entry is dampened, which is the invalid route. H indicates the table entry history, which is not a ture route and is the invalid route. "* "indicates the table entry is valid, which can be chosen as the best route. " > "indiates the table entry is the best entry to use for that network. "I" indicates the table entry was learned via an internal BGP (iBGP) session

Origin codes indicates the origin of the entry. I is the entry originated from an Interior Gateway Protocol (IGP). E is the entry originated from an Exterior Gateway Protocol (EGP). ? is the origin of the path is not clear

For each route, display its status, destination address, gateway address, metric (MED), Local-preference, Weight, AS Path and other attributes. The gateway address of the locally generated route is 0.0.0.0. **Metric** is not displayed if it is not set. Local-preference is 100 by default for IBGP routes, and the default value is included if it is not displayed, or the set value is displayed. **Weight** is 32768 for locally generated routes, or 0 if not set. The **AS Path** field displays the AS Path attribute of the route, including the AS list and the Origin attribute. Enclosed in parentheses are AS-set or AS autonomous sub-systems.

The last line displays number of routes, including all valid and invalid routes

```
B3710_118#show ip bgp
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network Next Hop Metric LocPrf Weight Path
* 192.168.10.0/24 192.168.69.5 0 10 400 i
*>i192.168.10.0/24 192.168.69.14 100 0 (65030) 400 i
*>i192.168.11.0/24 192.168.69.14 100 0 (65030) 400 i
* 192.168.65.0/30 192.168.69.1 100 0 (65020) 10 ?
*> 192.168.65.0/30 192.168.69.5 0 10 ?
* 192.168.65.4/30 192.168.69.1 100 0 (65020) 10 ?
*> 192.168.65.4/30 192.168.69.5 0 10 ?
* 192.168.65.8/30 192.168.69.1 100 0 (65020) 10 ?
*> 192.168.65.8/30 192.168.69.5 0 10 ?
* 192.168.66.0/30 192.168.66.2 100 0 (65020) ?
*> 192.168.66.0/30 0.0.0.0 32768 ?
* i192.168.66.4/30 192.168.66.6 100 0 ?
*> 192.168.66.4/30 0.0.0.0 32768 ?
*>i192.168.66.8/30 192.168.66.6 100 0 ?
*>i192.168.67.0/30 192.168.69.18 200 100 0 500 ?

Number of displayed routes: 15
```

Related commands

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

62.59 show ip bgp community

Syntax

To display statistics of BGP community structure, use the **show ip bgp community** command

show ip bgp community

Parameter

none

Command mode

exec

Usage guidelines

This command is used to display statistics information of BGP communities attribute structure in the system

Related commands

show ip bgp

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

62.60 show ip bgp ipv6 unicast

Syntax

To show the entry in ipv6 BGP routing table, run the following command

show ip bgp ipv6 unicast[**network**]

Parameter

Parameter	Description
network	Show the designated routing information

Command mode

Exec

Usage guidelines

The whole ipv6 BGP routing table is shown if the network is not designated. Details of the network is only shown if the network is designated

Example

The following is display information of a group of BGP. The front two rows show some tag information

Status code describes definition of the tag in front of the route. S represents suppression, which indicates the route is suppressed by the aggregation configuration and is an invalid route which will not be selected; d represents attenuation, which indicates the route is suppressed by the fluctuation and is an invalid route; h represents the historic route, which represents the route is saved as of the attenuation control and there is no a real route but only an invalid route. * represents a valid route, which indicates the route is valid and can be selected as the best route; > represents the best route, which indicates the best route slected from the valid routes; I represents the inner route, which indicates the route is from IBGP neighbor, which does not include routes from the sub-autonomous system of the autonomous league

Origin codes describes the Origin of the route, i means IGP, e means EGP, ? means indefinite

The command shows the attributes including the status, destination addres, gateway address, Metric(MED), Local-preference, Weight and AS Path of every route. The gateway address of the local route is 0.0.0.0. Metric is not shown if it is not configured with a definite setting. Local-preference for IBGP route is 100 by default; it includes the default value even if it is not shown or it is shown with the set value. Weight is 32768 or the set value; if it is not configured, it is 0. AS Path domain shows the attribute of AS Path, including AS list an Origin attribute. In the brackets is AS-set or sub-autonomous system of the autonomous system league

The last row shows the number of routes shown altogether, including valid and invalid routes

Related command

None

62.61 show ip bgp neighbors

Syntax

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the show ip bgp neighbors command

show ip bgp neighbors [*ip-address*] [**received-routes | routes | advertised-routes**]

Parameter

parameter	description
ip-ddress	IP address of a neighbor. If this parameter is omitted, information about all neighbors is displayed
received-routes	Displays all received routes (both accepted and rejected) from the specified neighbor
routes	Displays all routes that are received and accepted
advertised-routes	Displays all routes that have been advertised to neighbors

Command mode

EXEC

Usage guidelines

With this command, you can see detailed information and current status of neighbors, and you can also see some configuration information. By specifying the corresponding keywords, you can display the routes related to the neighbor

Related commands

show ip bgp

show ip bgp community

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

62.62 show ip bgp paths

Syntax

To display all the BGP paths in the database, use the show ip bgp paths command

show ip bgp paths

Parameter

none

Command mode

EXEC

Usage guidelines

This command is used to display statistics information of BGP paths structure

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

62.63 show ip bgp prefix-list

Syntax

To display ipv4 BGP routing information matching the specified prefix-list, use the **show ip bgp prefix-list** command

show ip bgp prefix-list {*prefix-list name*}

Parameter

parameter	description
prefix-list name	Name of prefix-list

Command mode

EXEC

Usage guidelines

This command specifies prefix-list to filter display of the show ip bgp command. Only the routes matching the prefix-list will be displayed

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

62.64 show ip bgp regexp

Syntax

To display routes matching the autonomous system path regular expression, use the show ip bgp regexp command

show ip bgp regexp *regular-expression*

Parameter

parameter	description
regular-expression	Regular expression to match the BGP autonomous system paths

Command mode

EXEC

Usage guidelines

This command specifies the regular expression to filter the display of the show ip bgp command. Only the routes matching the regular expression will be displayed

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

62.65 show ip bgp summary

Syntax

To display the status of all Border Gateway Protocol (BGP) connections, use the show ip bgp summary command

show ip bgp summary

Parameter

This command has no parameters or keywords

Command mode

EXEC

Usage guidelines

Some global configurations about the BGP protocol can be viewed through the **show ip bgp summary** command. Such as global **distance** configuration, **IGP** synchronization configuration, autonomous system alliance identification number, autonomous system alliance member, route reflection cluster identification, etc. In addition, the local autonomous system number, local router-id, and general information of all neighbors can also be seen through this command

Example

The following is sample output from the show **ip bgp summary** command:

router bgp 4

BGP local AS is 4

Router ID is 192.168.20.72

IGP synchronization is enabled

Distance: external 20 internal 200

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/Pref

192.168.20.12 4 5 0 0 0 0 0 never Connect

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

62.66 synchronization

Syntax

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the **synchronization** command. Use the no form of this command to disable this function

synchronization

no synchronization

Parameter

none

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

IGP synchronization means that when BGP receives a route from IBGP, whether it needs to wait until the route appears in the routing table in the form of IGP before advertising the route to other EBGP neighbors. When IGP synchronization is enabled, BGP must wait until the IBGP route appears in IGP to advertise to other EBGP neighbors; when IGP synchronization is not disabled, BGP will advertise to other EBGP neighbors when it receives IBGP routes. The IGP includes direct routes, static routes, RIP routes, OSPF routes, and other internal gateways protocol routing

IGP function is disabled by default.

Example

The following example enables switch to advertise the ibgp route after waiting for IGP synchronization

router bgp 120

synchronization

Related commands

router bgp

62.67 table-map

Syntax

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command. To disable this function, use the no form of the command

table-map <*name*>

no table-map

Parameter

parameter	description
name	Route map name from the route-map command

Default value

none

Command mode

BGP configuration mode

Usage guidelines

By setting the table-map, you can filter or modify attributes when BGP adds entries to the routing table

Example

none

Related commands

none

62.68 timers

Syntax

To modify the default timers of BGP neighbors,, use the timers bgp command. To reset the BGP timing defaults, use the no form of this command

timers bgp <*keepalive*> <*holdtime*> [*Idleholdtime*]

no timers bgp

Parameter

parameter	description
keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer
holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead
Idleholdtime	Default Idlehold interval of BGP neighbor

Default value

Keepalive:30 seconds

Holdtime:90 seconds

Idleholdtime: 0

Command mode

BGP configuration mode

Usage guidelines

Configure BGP neighbor clock in global configuration mode to modify default clock configuration. The configuration towards neighbor is prior to global configuration

Example

The following example changes the keepalive timer to 10 seconds and the hold-time timer to 40 seconds:

router bgp 100

timers bgp 10 40

Related commands

neighbor timers

Chapter 63 Public Routing Configuration Commands

63.1 Ip aspath-list Configuration Commands

63.1.1 ip as-path access-list

Syntax

To create the as-path list, run **ip as-path access-list**. To cancel the configured as-path list, run **no ip as-path access-list**

ip as-path access-list <*name*> <**deny | permit**> <*regexp*>

no ip as-path access-list <*name*> [**deny | permit**] [*regexp*]

Parameter

Parameter	Description
name	Name of the as-path list
deny | permit	Attribute of the as-path list
regexp	Regular expression of the as-path

Default value

All as-path expressions except those having a clear explanation on the **permit** regulation are declined by default

Command mode

Global configuration mode

Usage guidelines

The AS-path list is used to filter the AS-PATH attribute of the BGP route. The AS-PATH attribute of the BGP route is a number sequence which is expressed in form of the character string. The number at the right end is the autonomous system number for the route starting, while the numbers leftwards in turn are the numbers of the autonomous systems which the BGP route passes. For example, character string 22 23 98 means that the BGP route is transmitted from autonomous system 98, passes through autonomous system 23 and autonomous system 22, and finally reaches the local autonomous system

The AS-path list in the system is identified with the name. The total number of AS-path lists which are allowed to configure in the system is limited by the resource of the system. The same AS-path list can be configured with multiple matchup regulation. The procedure to apply the AS-path list is to check whether the matchup is successful or not according to the configuration order. Once a matchup is found to be successful, the following check-up will be stopped and the nature of the regulation (deny/permit) is then returned. If the matchup of all regulations is not successful, the nature of the regulation, **deny**, will be returned. Each regulation is organized according to their configuration order

The as-path expression is normally the regular expression. The special characters which are always used in the expression are shown in the following table:

Character	Symbol	Meaning
Full stop	.	Matches any single character, including space
Asterisk	*	Matches the 0 sequence or more sequences
Plus	+	Matches the 1 sequence or more sequences
Question mark	!	Follows the number 0 or 1
Addition character	^	Starting point of the matchup character string
Dollar	$	End point of the matchup character string
Underline	_	Matches these symbols: “,”, “{ }”, “( )”, “^”, “$” and “space”
Square bracket	[ ]	Stands for the range of the single-character mode
Hyphen	-	Separates a range

With the aid of the presentation methods of the AS-PATH attribute, the correct usage of the regular expression can help create the powerful AS-path list. The following examples are given:

.*	Representing any attribute of the AS path
^$	Representing the attributes of the null path
^22$	Representing the path attributes of autonomous system 22
^22_	Representing the path attribute starting with 22
_22$	Representing the path attribute starting with 22, such as 22, 34 22 and 99 45 22
_22_	R epresenting the path attribute containing 22, like 23 22 45 and 442 22 23 44

The **as-path list** command can be used together with the **match as-path** command and the **neighbor filter-list** command

Example

In the following example, the defined **as-path list hell** command permits all path attributes starting with 23 or containing 22:

ip as-path access-list hell permit ^23

ip as-path access-list hell permit _22_

Or:

ip as-path access-list guangzhou deny ^300

ip as-path access-list guangzhou deny _300_

ip as-path access-list guangzhou permit .*

The AS-PATH attributes starting with 300 or containing 300 will be declined, while other AS-PATH attributes can pass. If the defined order is different, the results will be totally different. The following AS-PATH attributes can pass.

ip as-path access-list guangzhou permit .*

ip as-path access-list guangzhou deny ^300

ip as-path access-list guangzhou deny _300_

Related command

match as-path

neighbor filter-list

63.2 show ip aspath-list

Syntax

To display the AS-path list configured in the system, run the following command:

show ip as-path-list [*name*]

Parameter

Parameter	Description
name	Name of the as-path list

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the as-path list is not designated, all configured as-path lists in the system will be displayed

Example

The following example shows that all as-path lists in the system will be displayed:

show ip as-path-list

Related command

ip as-path access-list

63.3 ip community-list Configuration Commands

63.3.1 ip community-list

Syntax

To create the regulations for the community list of the BGP route, run **ip community list**. To cancel the regulations for the community list, run **no community list**

ip community-list {**expanded | standard**} <*name*> {**deny | permit**} [**aa:nn | *1-4294967295* | local-AS | no-advertise | no-export**]

no ip community-list {**expanded | standard**} <*name*> {**deny | permit**} [**aa:nn | *1-4294967295* | local-AS | no-advertise | no-export**]

Parameter

Parameter	Description
name	Name of the community list
deny | permit	Attribute of the community list
<1-4294967295>	Value of the community, which is a 32-bit integer
aa:nn	New form of the community value aa stands for a 16-bit value. nn stands for the next 16-bit value
no-advertise	Means that no neighbor will be reported
local-AS	Means that the EBGP neighbor outside of the local autonomous system or in the same autonomous system ally will not be reported
no-export	Means that the neighbors in the local autonomous system or the autonomous system ally will not be reported

Default value

All communities except those having a clear explanation on the **permit** regulation are declined by default

Command mode

Global configuration mode

Usage guidelines

The community list is used to filter or set the community attribute of the BGP route. The community attribute is a group number or a community group number. A community number is a 4-byte value. The community numbers between 0x00000000 and 0x0000FFFF or between 0xFFFF0000 and 0xFFFFFFFF are reserved. These community numbers are globally accepted. The frequently-used community numbers are the following ones:

NO_EXPORT (0xFFFFFF01): After the route with this community number is received, the peers outside the autonomous system or autonomous system ally will not be reported

NO_ADVERTISE(0xFFFFFF02): After the route with the community number is received, no peers will be

reported

NO_EXPORT_SUBCONFED (0xFFFFFF03): It is always called as LOCAL_AS. After the route with the community number is received, the peers outside the local autonomous system are not reported

The community list in the system is identified by a name. The total number of the community lists which can be configured in the system is limited by the system's resource. The same community list can be configured with multiple matchup regulations. The procedure to apply the community list is to check whether the matchup is successful or not according to the configuration order. Once a matchup is found to be successful, the following check-up will be stopped and the nature of the regulation (deny/permit) is then returned. If the matchup of all regulations is not successful, the nature of the regulation, **deny**, will be returned. The order to check each regulation is the configuration order

One community-list regulation has three elements: name, regulation's attribute (deny/permit) and community number sequence. The community number sequence is a set of a group of community numbers. If all community numbers in the community attribute are in the community sequence with designated regulations, the matchup is successful. If not, the matchup fails and the next regulation will be matched

The **community list** command can be used together with commands **route-map** and **match community**

Example

In the following example, the community will be declined by the **ip community-list yall** command if the value of the community is 5 or 10; the community will be accepted by the **ip community-list yall** command if the value of the community is 15 or 20

ip community-list standard yall deny 5 10

ip community-list standard permit 15 20

Related command

match community-list 4

63.3.2 show ip community-list

Syntax

To display the community list configured in the system, run the following command:

show ip community-list <*name*>

Parameter

Parameter	Description
name	Name of the community list

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the community list is not designated, all configured community lists in the system will be displayed

Example

The following example shows that all community lists in the system will be displayed:

Show ip community-list

Related command

ip community-list

63.4 ip prefix-list commands

63.4.1 clear ip prefix-list

Syntax

To delete the statistics information about the designated prefix list, run the following command:

clear ip prefix-list [<name> [<*prefix*>]]

Parameter

Parameter	Description
name	Name of the prefix list
prefix	Network prefix which is in the A.B.C.D/n format n here stands for the length of the mask

Default

None

Command mode

EXEC

Usage guidelines

If the prefix is not designated, all statistics information in the prefix list will be canceled

Example

None

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

63.4.2 ip prefix-list

Syntax

To establish a prefix list or add a prefix-list regulation, run **ip prefix-list**. To cancel the configuration, run **no ip prefix-list**.

ip prefix-list <*name*> [<**seq**> <*seq_number*>] <**deny | permit**> <**prefix | any**> [<*ge*> <*value*>] [<**le**> <*value*>]

no ip prefix-list <*name*> [<**seq**> <*seq_number*>] <**deny | permit**> <**prefix | any**> [<*ge*> <*value*>] [<**le**> <*value*>]

Parameter

Parameter	Description
name	Name of the prefix list
seq	Designates the sequence number
seq_number	Value of the sequence number
deny | permit	Attribute of the prefix list
prefix | any	Designated prefix or any prefix
ge	Designates the minimum length of the matched prefix
value	Length of the prefix which ranges from 0 to 32
le	Designates the maximum length of the matched prefix
value	Length of the prefix which ranges from 0 to 32

Default value

None

Command mode

Global configuration mode

Usage guidelines

The prefix list is a set of regulations for filtrating the network prefix. Each regulation has five elements: sequence, deny/permit, prefix and length (a.b.c.d/n), upper limitation (le y) and bottom limitation (ge x). All regulations are sorted according to the sequence. When the prefix list is applied, the regulation of the smallest sequence is first checked. If the matchup is successful, other regulations stop the matchup operation and the matched regulation's attribute (deny/permit) is returned

When you check whether a regulation matches a designated network prefix, you should not only check the length of the network prefix but also check whether the network prefixes have the same length in the designated length. For example, to check whether a regulation of a prefix list, **ip prefix-list test seq 5 A.B.C.D/M ge X le Y**, matches the designated network **a.b.c.d/n**, the following procedure will be taken

Firstly, check whether the mask length of the network (n) meets the requirement of the expression: X <= n <= Y (if **ge X** is not designated, the expression is **M <= n<= Y**; if the **le Y** is not designated, the expression is **X <=n <= 32**; if both **ge X** and **le Y** are not designated, the expression is **n == M**). If the mask length meets the requirements of the expression, the next operation will be performed. If the mask length does not meet the regulation, the following regulation will be used

Check whether network a.b.c.d/n and the first M bit of A.B.C.D are same. If they are same, the regulation is met and the attribute of the regulation is returned; if the regulation is not met, the next regulation will be seen whether it is met

If all regulations are not met, the **deny** attribute will be returned

Regarding the sequence number of the prefix list, there is another command: **ip prefix-list sequence-number**. This command is used to control whether the prefix list uses the sequence number. For details, please refer to the description of this command

The no form of the command specifying only the name will delete the entire prefix list

Example

The following are destination routes and prefix lists:

Destination route 1:120.120.0.0/14

Destination route 2:120.120.0.0/16

Destination route 3:120.120.0.0/25

Destination route 4:130.130.0.0/16

Destination route 5:130.130.0.0/8

Destination route 6:130.130.0.0/24

Destination route 7:12.0.0.0/8

Prefix-list:
ip prefix-list sample permit 120.120.0.0/8 ge 16 le 24
ip prefix-list sample deny 130.130.0.0/16

The following are the matchup results:

Destination route 1: unsuccessful, deny

Destination route 2: successful, permit

Destination route 3: unsuccessful, deny

Destination route 4: successful, deny

Destination route 5: unsuccessful, deny

Destination route 6: unsuccessful, deny

Destination route 7: unsuccessful, deny

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

63.4.3 ip prefix-list description

Syntax

To configure the description of the prefix list, run **ip prefix-list**. To cancel the description of the prefix list, run **no ip prefix-list**

ip prefix-list <*name*> <**description**> <*strings*>

no ip prefix-list <*name*> <**description**>

Parameter

Parameter	Description
name	Name of the prefix list
description	Designates the description information of the prefix list
strings	Description information

Default value

None

Command mode

Global configuration mode

Usage guidelines

None

Example

The following example shows how to add the description information to **prefix-list hard** for convenient reading:

ip prefix-list hard deny any

ip prefix-list hard description This prefix-list is used to filter routes from neighbor hard

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

63.4.4 ip prefix-list sequence-number

Syntax

To enable the prefix list to use the sequence, run **ip prefix-list** ***sequence-number***. To cancel the sequence, run **no ip prefix-list** ***sequence-number***

ip prefix-list sequence-number

no ip prefix-list sequence-number

Parameter

None

Default value

The sequence is used by default

Command mode

Global configuration mode

Usage guidelines

The command is used to decide whether each regulation of the prefix list has been allocated with a sequence. After the sequence is used, the same sequence corresponds to only one regulation. Hence, if a regulation with a same sequence is newly generated, the previously old regulation will be deleted. If the sequence is not used, you have to run a command to delete the regulation. The sequence may not be designated during configuration. The system then allocates the sequence for all regulations. The sequence starts from 5 and adds 5 each time

Example

None

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

63.4.5 show ip prefix-list

Syntax

To display the information about the prefix list or all prefix lists, including the configuration information and statistics information about the prefix list, run the following command:

show ip prefix-list [<**summary | detail**> <*name*>]

Parameter

Parameter	Description

summary	Summary information
detail	Detailed information
name	Name of the prefix list

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the prefix list is not designated, all information about the prefix list will be displayed

Example

The following example shows that a prefix list is configured

ip prefix-list yell permit 130.12.19.0/24

ip prefix-list yell permit 140.20.0.0/16 ge 16 le 24

The following information is shown after the **show ip prefix-list detail** command is run:

Prefix-list with the last deletion/insertion: yell

ip prefix-list yell: 2 entries

count: 2, range entries: 1, sequences: 5 - 10

seq 5 permit 130.12.19.0/24 (hit count: 0, refcount: 10)

seq 10 permit 140.20.0.0/16 ge 16 le 24 (hit count: 0, refcount: 10)

The first information line indicates that the recently-modified prefix list is **yell**

Starting from the second information line, all information about the prefix list is listed. Here only one prefix list is configured, whose name is **yell**

Count: 2, indicating that the prefix list has two options

Range entries: 1, indicating that the number of network range defined in the prefix list is 1

Sequences: 5-10, indicating the sequence range of each option in the prefix list

The following are the definition of each option and the statistics information

Hit count: 0, indicating that the times of option matchup is 0

Refcount: 10, meaning that the times of option matchup are 10

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

63.5 route-map Commands

63.5.1 route-map

Syntax

To create a route map or define a route-map item, run **route-map**. To delete the created route map or the defined route-map item, run **no route-map**

route-map *name* [*seq*] [**deny** | **permi**]

no route-map *name* [*seq*] [**deny** | **permi**]

Parameter

Parameter	Description
name	Name of the route map
seq	Sequence of the route map whose default value is 0
**deny	permit**	Attribute of the route map whose default value is **permit**

Default value

By default, the value of the **seq** parameter is 10 and the attribute is **permit**

Command mode

Global configuration mode

Usage guidelines

The route map is used to modify the route's attribute or the filtration route. The route map is always used for the strategy of the dynamic routing protocol, such as redistribute route, filtration route, setting the route's attribute for strategic routing, and so on

The same route map may have multiple items. The total number of the route map in the system is limited by the system's resource. Each item in the same route map can be designated with the sequence or the system will automatically generate the sequence for each item. Each item has a kind of attribute (deny/permit); each item can be conducted with the matchup regulation (match), regulations (set) and exit strategies (on-match)

Tue matchup regulation is used to check whether a feature of an object meets a certain rule. If the object meets all matchup regulations in the item, the object matches the item successfully, or the item matchup fails. If an item is not configured with the matchup regulation, any object cannot match the item. If the matchup regulation adopts other lists such as the access list, prefix list, community list or as-path list to check whether an object is matched, the returned value of the list is the result of regulation matchup

The setting regulation is used to set an attribute of an object. If an object matches the item successfully and the attribute of the item is **permit**, the setting regulations configured under the item are used to modify the attribute of the object. If the object matches the item and the attribute of the item is **deny**, the exit strategy will be checked. If the object fails to match the item, the next item matchup will be conducted until the matchup succeeds

The exit strategy decides the actions after the object matches the item successfully. If an object matches an item successfully and the item have not configured with the exit strategy, the checking to other items will be stopped and the attribute of the item (deny/permit) will be returned. If **on-match next** is configured, the checking on the next item will be continued. If **on-match goto N** is configured, the designated item, item N, will be the first one to be checked; if the designated item does not exist, the attribute of the item (deny/permit) will be returned

Under the same item, only one matchup regulation of the same attribute or the settings regulation can be configured. The following matchup regulation or settings regulation configured will replace the previous one. The following configuration can be done for the same item:

match metric 34

set metric 100

In the previous example, there is only one **match** regulation and the **set** regulation

To realize multiple values for matching the same attribute, you can use the exit regulations

route-map match-multi-metric 10 permit

match metric 10

on-match goto 30

route-map match-multi-metric 20 permit

match metric 20

on-match goto 30

route-map match-multi-metric 30 permit

set metric 100

In the same example, the route whose metric is 10 or 20 is matched and its metric will be set to 100

During configuration, the system can automatically generate a sequence for each item, starting from 10 by default and then adding 10 in turn. When the route map is applied, the system will check the sequence of the item from small to big

The route map can handle different types of routes, some **match** regulations and **set** regulations only suitable for parts of routes. If you try to use the unsupported **match** regulations or **set** regulations to match or modify the objects, the system will omit these regulations

If there is no name behind the **no route map** command, the whole route map will be deleted, or the designated item will be deleted

Example

The following example shows the route map is used to filter the routes forwarded by OSPF and to set the relative attributes

router bgp 20

redistribute ospf 3 route-map redist-ospf

route-map redist-ospf

match tag 139009

set local-preference 300

Related command

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.2 match as-path

Syntax

To set a **match** regulation of the route map and check the attributes of the BGP route through the AS-path map, run **match as-path**. To delete the configuration you have just done, run **no match as-path**

match as-path <*as-path-list-name*>

no match as-path <*as-path-list-name*>

Parameter

Parameter	Description
as-path-list-name	Name of the as-path list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The designated AS path list is used to match the object or to filter the AS-PATH attribute of the BGP route

Example

The following example shows how to check the whether the BGP route is matched using as-list1.

route-map match-aspath

match as-path as-list1

Related command

route-map

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.3 match community

Syntax

To set a **match** regulation of the route map and check the attributes of the BGP route through the community list, run **match community**. To delete the configuration you have just done, run **no match community**

match community <*community-list-name*>

no match community <*community-list-name*>

Parameter

Parameter	Description
community-list-name	Name of the community list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The designated community list is used to match the object and to filter the community attribute of the BGP route

Example

The following example shows how to check the whether the BGP route is matched using **as-list1**

route-map match-comm

match community comm-list1

Related command

route-map

match as-path

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.4 match ip address

Syntax

To set a route-map **match** regulation and match the destination network's address, run **match ip address**. To delete the configuration you have just done, run **no match ip address**

match ip address <*name*>

no match ip address <*name*>

Parameter

Parameter	Description
name	Name of the IP access list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The access list is used to filter the network address of the route, which is suitable for all IP routes and packets

Example

In the following example, the route checked by the access list is set to metric

route-map set-metric

match ip address acl-metric

set metric 100

Related command

route-map

match as-path

match community-list

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.5 match ip next-hop

Syntax

To set a route-map **match** regulation and check whether the next hop address of the route matches with the address of the designated next hop, run **match ip next-hop <*a.b.c.d*>**. To delete the configuration you have just done, run **no match ip next-hop <*a.b.c.d*>**

match ip next-hop <*a.b.c.d***>**

no match ip next-hop <*a.b.c.d***>**

Parameter

Parameter	Description
a.b.c.d	IP address

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The access list is used to check the attribute of the next hop, which is suitable for all IP routes

Example

In the following example, the route with the next hop's address 192.121.13.28 matches item 20 of the route map

route-map beijing 10 permit

match ip nexthop 172.12.29.98

set metric 100

route-map beijing 20 permit

match ip nexthop 192.121.13.28

set metric 20

Related command

route-map

match as-path

match community-list

match ip address

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.6 match ip address prefix-list

Syntax

To set a route-map **match** regulation and match the destination network's address, run **match ip address prefix list**. To delete the configuration you have just done, run **no match ip address prefix-list**

match ip address prefix-list <*name***>**

no match ip address prefix-list <*name***>**

Parameter

Parameter	Description
name	Name of the prefix list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes

Example

The following example shows that the route whose destination address is 192.121.0.0 matches **route-map match-prefix**

ip prefix-list beijing permit 192.121.0.0/16

route-map match-prefix

match ip address prefix-list beijing

set metric 100

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.7 match length

Syntax

To set a route-map **match** regulation and check whether the route's metric matches the address of the designated metric, run **match length**. To delete the configuration you have just done, run **no match length**

match length <*minimum-length*> <*maximum-length*>

no match length <*minimum-length*> <*maximum-length*>

Parameter

Parameter	Description
minimum-length	Minimum length of the packet
maximum-length	Maximum length of the packet

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route

Related command

route-map

63.5.8 match metric

Syntax

To set a route-map **match** regulation and check whether the route's metric matches the address of the designated metric, run **match metric <*value*>**. To delete the configuration you have just done, run **no match metric <*value*>**

match metric <*value***>**

no match metric <*value***>**

Parameter

Parameter	Description
value	Metric value

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all routes

Example

The following example shows that the routes whose metric values are 120 are declined because they match item 20 of the route map

route-map beijing 10 permit

match ip nexthop 172.12.29.98

set metric 100

route-map beijing 20 deny

match metric 120

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.9 match tag

Syntax

To set a route-map **match** regulation and check whether the route's tag matches the designated tag, run **match tag <*value*>**. To delete the configuration you have just done, run **no match tag <*value*>**

match tag <*value*>

no match tag <*value*>

Parameter

Parameter	Description
value	Value of the Tag

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all routes

Example

The following example shows that the routes whose tags' values are 120923 are declined because they match item 20 of the route map

route-map huang 10 permit

match ip nexthop 172.12.29.98

set metric 100

route-map huang 20 deny

match tag 120923

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.10 on-match

Syntax

To configure the exit strategy of the route-map item, run **on-match**. To cancel the configuration, run **no on-match**

on-match {**next** | **goto** *n*}

no on-match {**next** | **goto** }

Parameter

Parameter	Description
n	Sequence of the item

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The command is used to configure the exit strategy of the route-map item. If a route-map item is successfully matched and the item have not configured with the exit strategy, the checking to other items will be stopped and the attribute of the item (deny/permit) will be returned. If **on-match next** is configured, the checking on the next item will be continued. If **on-match goto N** is configured, the designated item, item N, will be the first one to be checked; if the designated item does not exist, the attribute of the item (deny/permit) will be returned

Example

None

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.11 set aggregator

Syntax

To configure a route-map setting regulation and set the BGP route to **aggregator**, run **set aggregator**. To delete the configuration you have just done, run **no set aggregator**

set aggregator as <*as-number*> <*a.b.c.d*>

no set aggregator as <*as-number*> <*a.b.c.d*>

Parameter

Parameter	Description

as-number	Number of the autonomous system of the route aggregator
a.b.c.d	IP address of the route aggregator

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route

Example

The following example shows that all routes are set to **aggregator**

route-map huang

set aggregator as 200 192.12.90.82

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.12 set as-path

Syntax

To configure a route-map setting regulation and add AS before the **as-path** attribute of the BGP route, run **set as-path prepend**. To delete the configuration you have just done, run **no set as-path prepend**

set as-path prepend <*as*>

no set as-path prepend <*as*>

Parameter

Parameter	Description
prepend	Means that AS is added before the as-path attribute
as	Number of the autonomous system

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route

Example

In the following example, the length of the **as-path** attribute is added by adding the autonomous system number before the **as-path** attribute for each route and the result of routing choice is herein changed

route-map add-as

set as-path prepend 200 200 200 200

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.13 set atomic-aggregate

Syntax

To configure a route-map setting regulation and set the BGP route to **aggregator**, run **set atomic-aggregate**. To delete the configuration you have just done, run **no set atomic-aggregate**

set atomic-aggregate

no set atomic-aggregate

Parameter

None

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route. If the aggregation of information loss is generated when a system transmits the route, you need set the route to **atomic-aggregate**

Example

In the following example, the length of the **as-path** attribute is added by adding the autonomous system number before the **as-path** attribute for each route and the result of routing choice is herein changed

route-map tee

set atomic-aggregate

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.14 set community

Syntax

To configure a route-map setting regulation and set the BGP route to **community**, run **set community**. To delete the configuration you have just done, run **no set community**

set community <*aa:nn* / *1-4294967295* | **local-AS | no-advertise | no-export**>

no set community <*aa:nn* / *1-4294967295* | **local-AS | no-advertise | no-export**>

Parameter

Parameter	Description
aa:nn	Format of the community value
1-4294967295	Value range of the community parameter
no-advertise	Means that any neighbor will not be reported
local-AS	Means that the EBGP neighbor outside of the local autonomous system or in the same autonomous system ally will not be reported
no-export	Means that the neighbors in the local autonomous system or the autonomous system ally will not be reported

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route. The newly-set community attribute will replace the previous community attribute of the route

Example

In the following example, all routes from neighbor 193.12.202.12 will be set to **local-AS community**, enabling these routes not to be reported to other autonomous systems

router bgp 200

neighbor 193.12.202.12 remote 100

neighbor 193.12.202.12 route-map tee in

route-map tee

set community local-AS

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.15 set community-additive

Syntax

To configure a route-map setting regulation and add a value to the community attribute of the BGP route, run **set community-additive**. To delete the configuration you have just done, run **no set community-additive** <*aa:nn* / *1-4294967295* | **local-AS | no-advertise | no-export**>

set community-additive <*aa:nn* / *1-4294967295* | **local-AS | no-advertise | no-export**>

no set community-additive <*aa:nn* / *1-4294967295* | **local-AS | no-advertise | no-export**>

Parameter

Parameter	Description
aa:nn	Format of the community value
1-4294967295	Value of the community parameter
no-advertise	Means that any neighbor will not be reported
local-AS	Means that the EBGP neighbor outside of the local autonomous system or in the same autonomous system ally will not be reported
no-export	Means that the neighbors in the local autonomous system or the autonomous system ally will not be reported

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route. The newly-set community attribute will be added to the previous community attribute of the route

Example

In the following example, all routes from neighbor 193.12.202.12 will be set to **local-AS community**, enabling these routes not to be reported to other autonomous systems

router bgp 200

neighbor 193.12.202.12 remote 100

neighbor 193.12.202.12 route-map tee in

route-map tee

set community-additive local-AS

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.16 set default

Syntax

To set the default information for the strategy route, run **set default interface**. To cancel the configuration, run **no set default interface**

set default interface<*interface-name*> [load-balance]

no set default interface <*interface-name*> [load-balance]

Parameter

Parameter	Description
interface-name	Name of the designated interface
load-balance	Allow port routing balance

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. The default outgoing interface of the strategy route is configured through the command. Only when the interface is in the use state can this command validate. The interface must meet two conditions before it is used

Firstly:The UP protocol is running on the interface

Second: The interface has the IP address or the negotiation IP address, or the interface is the NULL interface

Related command

route-map

63.5.17 set interface

Syntax

To set the outgoing interface for the strategy route, run **set interface**. To cancel the configuration, run **no set interface**

set interface <*interface-name*> [load-balance]

no set interface <*interface-name*> [load-balance]

Parameter

Parameter	Description
interface-name	Name of the designated interface
load-balance	Allow port routing balance

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. The default outgoing interface of the strategy route is configured through the command. Only when the interface is in the use state can this command validate. The interface must satisfy two conditions before it is used

Firstly:The UP protocol is running on the interface

Secondly: The interface has the IP address or the negotiation IP address, or the interface is the NULL interface

Related command

route-map

63.5.18 set ip default

Syntax

To set the default next hop for the strategy route, run **set ip default nexthop**. To cancel the configuration, run **no set ip default nexthop**

set ip default nexthop <*A.B.C.D*> [load-balance]

no set ip default nexthop <*A.B.C.D*> [load-balance]

Parameter

Parameter	Description
A.B.C.D	Gateway's address
load-balance	Allow route balancing for next hop

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. Only when the next hop arrives can this command be valid

Example

None

Related command

route-map

63.5.19 set ip precedence

Syntax

To set the precedence for the strategy route, run **set ip precedence <0-7>**. To cancel the configuration, run **no set ip precedence <0-7>**

set ip precedence <0-7>

no set ip precedence <0-7>

Parameter

Parameter	Description
0-7	Precedence which is set for the packet

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. When the suitable route is found by the strategy route for routing, the precedence can also be set. If the strategy route fails, the precedence cannot be set. The precedence of the IP packet is defined as follows:

routine0

priority1

immediate2

flash3

flash-override4

critical5

internet 6

network 7

Related command

route-map

63.5.20 set ip tos

Syntax

To set the tos for the strategy route, run **set ip tos**. To cancel the configuration, run **no set ip tos**

set ip tos <0-15>

no set ip tos <0-15>

Parameter

Parameter	Description
0-15	TOS which is set for the packet

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. When the suitable route is found by the strategy route for routing, TOS can also be set. If the strategy route fails, the TOS cannot be set. Different TOS' can be set according to their order or can be set together:

normal0

min-monestary1

max-reliability2

max-throughput4

min-delay8

Related command

route-map

63.5.21 set ip next-hop

Syntax

To configure a route-map setting regulation and set the next-hop address of the route, run **set ip next-hop**. To delete the configuration you have just done, run **no set ip next-hop**

set ip next-hop <*a.b.c.d*> [load-balance]

no set ip next-hop <*a.b.c.d*> [load-balance]

Parameter

Parameter	Description
a.b.c.d	IP address
load-balance	Set port load balancing

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes

Example

In the following example, the next-hop addresses of all routes from neighbor 193.12.202.12 are set to 193.12.202.1:

router bgp 200

neighbor 193.12.202.12 remote 100

neighbor 193.12.202.12 route-map tee in

route-map tee

set ip next-hop 193.12.202.1

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.22 set local-preference

Syntax

To configure a route-map setting regulation and set the local preference of the BGP route, run **set local-preference**. To delete the configuration you have just done, run **no set local-preference**

set local-preference <*value*>

no set local-preference <*value*>

Parameter

Parameter	Description
value	Value of the local preference

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route

Example

The following example shows that the route map can set **local-preference** to 200:

route-map set-local-pref

set local-preference 200

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set metric

set origin

set tag

set weight

show route-map

63.5.23 set metric

Syntax

To configure a route-map setting regulation and set the metric of the route, run **set metric**. To delete the configuration you have just done, run **no set metric**

set metric <*value*> [*BEIGRP-delay reliability loading MTU*]

no set metric <*value*> [*BEIGRP-delay reliability loading MTU*]

Parameter

Parameter	Description
value	Value of the metric
BEIGRP-delay	BEIGRP port delay (unit: 10ms). Range is from 0 to 4294967295
reliability	BEIGRP port reliability (255 means completely reliable). Range is from 0 to 255
loading	BEIGRP load parameters (255 represents full load). Range is from 0 to 255
MTU	BEIGRP port MTU. Range is from 0 to 4294967295

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes

Example

The following example shows that the route map can set metric to 120:

route-map set-metric

set metric 120

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set origin

set tag

set weight

show route-map

63.5.24 set metric-type

Syntax

To set the value of the metric-type parameter for supporting the external type OSPF route, run **set metric-type**. To delete the configuration you have just done, run **no set metric-type**

set metric-type [**type-1** | **type-2**]

no set metric-type [**type-1** | **type-2**]

Parameter

Parameter	Description
Type-1	External type-1 of OSPF metric
Type-2	External type-2 of OSPF metric

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to external OSPF routes

Example

The following example shows that the route map can set **metric-type** to **type1**:

route-map set-metric-type

set metric-type type-1

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

63.5.25 set origin

Syntax

To set the origin attribute of the BGP route, run **set origin**. To delete the configuration you have just done, run **no set origin**

set origin {**igp** | **egp** | **incomplete**}

no set origin {**igp** | **egp** | **incomplete**}

Parameter

Parameter	Description
igp	Internal route of the autonomous system
egp	External route of the autonomous system
incomplete	Uncertain route

Default value

Igp is he default route locally configured through the **network** command, **Incomplete** is the default route locally configured through the **aggregate** command or the **redistribute** command

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route

Example

The following example shows how the defined route map sets the BGP route with a 10-starting **original** attribute to **igp**

ip as-path-list self permit ^10
route-map set-origin
match as-path self
set origin igp

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set tag

set weight

show route-map

63.5.26 set tag

Syntax

To set the tag of the route, run **set tag**. To delete the configuration you have just done, run **no set tag**

set tag <*value*>

no set tag <*value*>

Parameter

Parameter	Description
value	Value of the tag

Default value

The default tag value is 0

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes

Example

The following example shows how to set **tag** to 120980 through the route map:

route-map set-tag

set tag 120980

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set weight

show route-map

63.5.27 set weight

Syntax

To set the weight of the BGP route, run **set weight**. To delete the configuration you have just done, run **no set weight**

set weight <*value*>

no set weight <*value*>

Parameter

Parameter	Description
value	Value of the weight

Default value

The default weight value of the locally-generated BGP route is 32768 and the weight value obtained from the neighbor is 0

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route

Example

The following example shows how to set the weight to 230 through the route map:

route-map set-weight

set weight 230

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

show route-map

63.5.28 show route-map

Syntax

To display the information about the route map, run the following command:

show route-map [*name*]

Parameter

Parameter	Description
name	Name of the route map

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the route map is not designated, all configured route maps in the system will be displayed

Example

The following example shows that all route maps in the system are displayed:

Show route-map

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

Chapter 64 PBR Configuration Commands

64.1 debug ip policy

Syntax

To check the results of applying the policy route, run **debug ip policy**. To return to the default setting, use the no form of this command

debug ip policy

no debug ip policy

Parameter

None

Default value

By default, the results of policy route application will not be printed

Command mode

EXEC

Usage guidelines

This command can be used to check whether the IP packets received from the interface have been applied with the policy route

Because the results of policy routing application for each interface-received IP packet will be printed after this command is run, please use this command when the network traffic is low

Example

The following example shows how to display the policy routing debug information

Router# debug ip policy

2004-1-16 15:32:54 PBR: s=10.1.1.2 (vlan1), d=99.1.1.1, len 84, policy rejected -- normal forwarding

2004-1-16 15:32:54 PBR: s=10.1.1.21 (vlan1), d=99.1.1.1 (vlan2), len= 84, gate=13.1.1.99 policy routed

Related command

None

64.2 ip policy route-map

Syntax

To apply the policy route to the interface-received IP packet, run **ip policy route-map route-map name** in interface configuration mode. To cancel the policy route on the interface, run **no ip policy route-map**

ip policy route-map *route-map name*

no ip policy route-map

Parameter

Parameter	Description
route-map name	Name of the route map

Default value

None

Command mode

Interface configuration mode

Usage guidelines

If you want to apply the policy route to the interface-received IP packet, you need to run the **ip policy route-map** command

Example

The following example shows how to enable the policy route on interface vlan1

Switch _config#int vlan1

Switch _config_v1#ip policy route-map pbr

Related command

route-map

64.2.1 match ip address

Syntax

To apply the matchup policy based on source IP address, run **match ip address** ***access-list name***

match ip address *access-list name*

no match ip address [*access-list name*]

Parameter

Parameter	Description
access-list name	Name of the standard IP access control list

Default value

The access list is not designated by default

Command mode

Route-map configuration mode

Usage guidelines

If the route map is applied to the policy route, the source address of the IP packet will be used to match the configured access list. If the source address does match the access list, the **set** regulation is then applied; otherwise, the next sequence number of the same route map will be used

Example

The following example shows that the packets whose source IP addresses are allowed by access list net1 will be transmitted to interface vlan2:

Interface vlan1

ip policy route-map moon

!

route-map moon

match ip address net1

set interface vlan2

Related command

set default interface

set interface

set ip default next-hop

set ip next-hop

route-map

64.2.2 match length

Syntax

To set the route policy according to the length of the IP packet, run **match length**

match length *minimum-length maximum-length*

no match length *minimum-length maximum-length*

Parameter

Parameter	Description
minimum-length	Designates the minimum length of the matched packet.
maximum-length	Designates the maximum length of the matched packet.

Default value

It is not configured by default

Command mode

Route-map configuration mode

Usage guidelines

This command is used to conduct the policy routing according to the size of the IP packet

Example

The following example shows that the IP packet whose size ranges between 1000 bytes to 1500 bytes will be transmitted to interface vlan2.

Interface vlan1

ip policy route-map moon

!

route-map moon

match length 1000 1500

set interface vlan2

Related command

match ip address

set default interface

set interface

set ip default next-hop

set ip next-hop

route-map

64.2.3 set default interface

Syntax

To set the default next-hop interface for the matched IP packet, run **set default interface**

set default interface *interface name* [*...interface name*] [**load-balance**]

no set default interface *interface name* [*...interface name*] [**load-balance**]

Parameter

Parameter	Description
interface name	Name of the interface

Default value

It is not configured by default

Command mode

Route-map configuration mode

Usage guidelines

Before you set the default next-hop interface for the matched IP packet through the set default interface command, the following conditions must be satisfied:

1.The **set ip next-hop** command is not configured, or the **set ip next-hop** command is configured but the route of the next hop designated by **set ip next-hop** is not in the routing table

2.If the **set interface** command is not configured or the **set interface** command is configure but these interfaces cannot be routed (the interface is down or there is no IP address).

3.The **set ip default next-hop** command or the **set ip default next-hop** command is not configured but the route of the next hop designated by **set ip default next-hop** is not in the routing table

Example

None

Related command

match ip address

match length

set interface

set ip default next-hop

set ip next-hop

route-map

64.2.4 set interface

Syntax

To set the next-hop interface for the matched IP packet, run **set interface**

set interface interface name [*...interface name*] [**load-balance**]

no set interface interface name [*...interface name*] [**load-balance**]

Parameter

Parameter	Description
interface name	Name of the interface

Default value

It is not configured by default

Command mode

Route-map configuration mode

Usage guidelines

Before you set the next-hop interface for the matched IP packet through the set interface command, the following conditions must be satisfied:

1.The **set ip next-hop** command or the **set ip next-hop** command is not configured, and the route of the next hop designated by **set ip next-hop** is not in the routing table

2.The interface is in the routing state (the protocol on the interface is up and the IP address exists)

Example

None

Related command

match ip address

match length

set default interface

set ip default next-hop

set ip next-hop

route-map

64.2.5 set ip default next-hop

Syntax

To set the default next-hop for the matched IP packet, run **set ip default next-hop**

set ip default next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

no set ip default next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

Parameter

Parameter	Description
A.B.C.D	Address of the next hop

Default value

It is not configured by default

Command mode

Route-map configuration mode

Usage guidelines

Before you set the default next hop for the matched IP packet through the **set ip default next-hop** command, the following conditions must be satisfied

1.The **set ip next-hop** command or the **set ip next-hop** command is not configured, and the route of the next hop designated by **set ip next-hop** is not in the routing table

2.If the **set interface** command is not configured or the **set interface** command is configure but these interfaces cannot be routed (the interface is down or there is no IP address).

3.The route of the next hop designated by the **set ip default next-hop** command exists in the routing table

Related command

set default interface

set interface

set ip next-hop

route-map

64.2.6 set ip next-hop

Syntax

To set the next hop for the matched IP packet, run **set ip next-hop**

set ip next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

no set ip next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

Parameter

Parameter	Description
A.B.C.D	Address of the next hop

Default value

It is not configured by default

Command mode

Route-map configuration mode

Usage guidelines

Before you set the next hop for the matched IP packet through the **set ip next-hop** command, the following conditions must be satisfied:
The route of the next hop designated by the **set ip next-hop** command exists in the routing table

Related command

set default interface

set interface

set ip default next-hop

set ip next-hop

route-map

64.2.7 route-map

Syntax

route-map *route-map name* [*sequence-number*] [**permit** | **deny**]

no route-map *route-map name* [*sequence-number*] [**permit** | **deny**]

Parameter

Parameter	Description
route-map name	Name of the route map
sequence-number	Sequence number of the designated route map, which is optional
permit	Means that the route or the policy route is allowed to be forwarded if the IP packet is matched. The parameter is optional
deny	Means that the route or the policy route is forbidden to be forwarded if the IP packet is matched. The parameter is optional

Default value

There is no static routes by default

Command mode

Global configuration mode

Usage guidelines

The **route-map** command is used to configure the route map

Example

The following example shows that route map **pbr** is configured

route-map pbr 10 permit

match ip address net1

set ip next-hop 13.1.1.99

!

route-map pbr 20 permit

match ip address net2

set ip next-hop 14.1.1.99

!

route-map pbr 30 permit

match ip address net3

set ip next-hop 13.1.1.99 14.1.1.99 load-balance

Related command

match ip address

match length

set default interface

set interface

set ip default next-hop

set ip next-hop

64.2.8 ip local policy

Syntax

To open the policy route of the local packet, run **ip local policy route-map [*name*]**. To shut down the policy route of the local packet, run **no ip local policy route-map [*name*]**

ip local policy route-map *name*

no ip local policy route-map *name*

Parameter

Parameter	Description
name	Name of the route map used by the policy route

Default value

The policy routing function of the local packet is shut down by default

Command mode

Global configuration mode

Usage guidelines

The policy route can be applied to the locally-transmitted packets or the forwarded packets. The route applied

to the locally-transmitted packets are called as the local policy route. After the **ip local policy route-map <*name*>** command and a proper route map are configured in global configuration mode, you can apply the policy route to the locally-transmitted packets

The policy route checks whether the packets are the broadcast packets, and the broadcast packets also checks the corresponding policy route. Among the results of the policy route, only an outgoing interface or a next hop is shown. The route-to-multiport condition does not exist

The route map which is used for the policy route can match the packet according to the access list or the packet's length. The policy routing is conducted by setting the next hop or the outgoing interface. Various policies can be satisfied using the access list according to the routes, such as the route of the source address and the application route

The policy route can be used to set the outgoing interface, next hop, TOS and precedence of the packet. The order to choose the policy route is as follows: nexthop, default nexthop, interface and default interface. The normal route can be adopted when all the four types of previous policy routes are unavailable

If **nexthop** is available, it means that a route can be found in the routing table for **nexthop**. If **interface** is available, it means that the IP protocol on the interface is up and the legal IP address exists

Example

The following example shows that the policy routing is conducted to the locally-transmitted packets. The packets from the network whose destination address is 100.0.0.0/8 will be transmitted to interface vlan1:

ip local policy route-map Policy

!

route-map Policy

match ip address Policy-ACL

set interface vlan1

!

ip access-list extended Policy-ACL

permit ip any 100.0.0.0 255.0.0.0

!

Related command

ip policy

show ip local policy

show ip policy

64.2.9 ip policy

Syntax

To open the policy route on an interface, run **ip policy route-map [*name*]**. To shut down the local policy route, run **no ip policy route-map [*name*]**

ip policy route-map *name*

no ip policy route-map

Parameter

Parameter	Description
name	Name of the route map used by the policy route

Default value

The policy routing function on an interface is shut down by default

Command mode

Port configuration mode

Usage guidelines

The policy route can be applied to the locally-transmitted packets or the forwarded packets

The policy route is to check whether the packet is the broadcast packet, while the broadcast packet is also to check the corresponding policy route

The route map which is used to match the policy route can match the packet according d to the access list or the packet's length. Various policy requirements can be satisfied through the usage of the access list, such as source-address-based routing and application-based routing

You can set the egress port, nexthop, tos and precedence for the policy route. When the policy route is used, the order to select the route is: set ip nexthop, set interface,non-default normal route, set ip default nexthop, set default interface, normal route or default route. The policy route can set tos and precedence uniquely for normal routes

The availability of nexthop means that the nexthop can be used to find a route in the routing table. The interface availability means that the IP protocol on the interface is up and the interface has a legal IP address

Example

The following example shows that the policy routing can be conducted to a packet received by interface vlan1 and the packet whose destination address is 100.0.0.0/8 can be transmitted to interface vlan2:

interface vlan1

ip policy route-map Policy

!

route-map Policy

match ip address Policy-ACL

set interface vlan2

!

ip access-list extended Policy-ACL

permit ip any 100.0.0.0 255.0.0.0

!

Related command

ip local policy

show ip local policy

show ip policy

64.2.10 ip route-weight

Syntax

To configure the route weight on an interface, run **ip route-weight**. To resume the original route weight on an interface, run **no route-weight**. The original value of the route weight is 1

ip route-weight [*value*]

no ip route-weight

Parameter

Parameter	Description
value	Route weight

Default value

The default value of the route weight is 1

Command mode

Port configuration mode

Usage guidelines

You can configure the **ip route-weight** command on an interface to realize rate-based flow distribution

At first, you need to configure the **ip route load-balance** command in global mode; then, you need to configure the route weight at the egress port of the equivalence route according to the flow distribution rate. In this way, the packet can be transmitted on different egress ports of the equivalence route according to the configured rate. In this case, you must disable the ip cache function

Example

The following example shows that the packet is transmitted at a rate of 3:2 on interface vlan1 and interface vlan2 after it arrives destination network 5.0.0.0.

Interface vlan1

ip route-weight 3

ip address 3.0.0.1 255.0.0.0

no ip directed-broadcast

!

interface vlan2

ip route-weight 2

ip address 8.0.0.1 255.0.0.0

no ip directed-broadcast

duplex half

!

ip route load-balance

ip route 5.0.0.0 255.0.0.0 FastEthernet0/0 1.2.3.5 2

ip route 5.0.0.0 255.0.0.0 Ethernet1/1 2.2.3.5 2

The route weight of interface vlan1 is set to 3, while the route weight of interface vlan2 is set to 2. If they are configured as 6 and 4 respectively, they will have the same effect. Their greatest common divisor is eliminated here

Related command

ip route load-balance

ip route-cache

64.2.11 show ip local policy

Syntax

show ip policy

Parameter

None

Default value

None

Command mode

EXEC mode

Usage guidelines

show ip local policy

The command is used to how to show the configuration status of local policy routing

Example

None

Related command

ip local policy

ip policy

show ip policy

64.2.12 show ip policy

Syntax

show ip policy

Parameter

None

Default value

None

Command mode

EXEC mode

Usage guidelines

The **show ip policy** command is used to display the configuration state of the policy route

Example

None

Related command

ip local policy

ip policy

show ip local policy

Chapter 65 Switch Routing Protocol Highpriority Configuration Commands

65.1 switch routing-protocol-highpriority

Syntax

To enable or disable set priority of the routing packets forwarding to CPU, run the following command. To return to the default setting, use the no form of this command

[no] switch routing-protocol-highpriority

Parameter

None

Default value

Disabled

Command mode

Global configuration mode

Usage guidelines

None

Example

The following example shows how to set priority of the routing packets forwarding to CPU

Switch _config# switch routing-protocol-highpriority

Switch _config#

Chapter 66 AAA Configuration Commands

66.1 aaa authentication banner

Synta

To configure the login banner, run the following command. To return to the default setting, use the no form of this command

aaa authentication banner delimiter string delimiter

no aaa authentication banner

Parameter

Parameter	Description
delimiter string delimiter	String shown when the user logs in. The delimiter is ""

Default

The default banner is:

User Access Verification

Command Mode

Global configuration mode

Usage Guidelines

To create a banner, you have to configure a delimiter and then the text character string. The delimiter is to notify the system that its following text character string will be shown as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is end

Example

The following example shows how to change the login banner to the following character string:

aaa authentication banner "Welcome to BDCOM system!"

Related Command

aaa authentication fail-message

66.2 aaa authentication fail-message

Syntax

To configure the failed-login banner, run the following command. To return to the default setting, use the no form of this command

aaa authentication fail-message delimiter string delimiter

no aaa authentication fail-message

Parameter

Parameter	Description
delimiter string delimiter	String shown when the user logs in. The delimiter is ""

Default

The default failed login banner:

Authentication failed!

Command Mode

Global configuration mode

Usage Guidelines

To create a banner, you have to configure a delimiter and then the text character string. The delimiter is to notify the system that its following text character string will be shown as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is end

Example

The following example shows how to change the failed-login banner to the following character string:

aaa authentication fail-message "See you later"

Related Command

aaa authentication banner

66.3 aaa authentication username-prompt

Syntax

To change the username prompt, run the following command. To return to the default setting, use the no form of this command

aaa authentication username-prompt text-string

no aaa authentication username-prompt

Parameter

Parameter	Description

text-string	Text shown when the username prompt appears

Default

The username prompt character string is "Username" when there is no defined text string

Command Mode

Global configuration mode

Usage Guidelines

The command "aaa authentication username-prompt" can be used to change the character string of the username prompt

Username:

Some protocols (such as TACACS+) are capable of overlapping the local user name prompt information. In this circumstance, command "aaa authentication username-prompt" doesn't change the character string of the user name prompt

Note:

The command **aaa authentication username-prompt** doesn't change any prompt information provided by remote TACACS+ or RADIUS server

Example

The following example shows how to change the character string of the username prompt to the following character string:

aaa authentication username-prompt "YourUsernam:"

Related Command

aaa authentication password-prompt

66.4 aaa authentication password-prompt

Syntax

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt global configuration command. Use the no form of this command to return to the default password prompt text

aaa authentication password-prompt text-string

no aaa authentication password-prompt

Parameter

Parameter	Description

test-string	String of text that will be displayed when the user is prompted to enter a password

Default

There is no user-defined text-string, and the password prompt appears as "Password:"

Command Mode

Global configuration mode

Usage Guidelines

Use the **aaa authentication password-prompt** command to change the default text that the software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The no form of this command returns the password prompt to the default value:

Password:

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server or RADIUS server

Example

The following example shows how to change the text of the username prompt to "Your Password:"

aaa authentication password-prompt "YourPassword:"

Related Command

aaa authentication username-prompt

enable password

66.4.1 aaa authentication dot1x

Syntax

To configure dot1x access authentication, run the following command. To return to the default setting, use the no form of the above command

aaa authentication dot1x {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication dot1x {**default** | *list-name*}

Parameter

Parameter	Description
Default	Use the authentication method following the Parameteras the default method
list-name	The character string used to name the authentication method list. The method in the authentication method list will be activated when the user accesses the authentication

method	At one keyword described by "dot1x authentication method"

Default

The authentication return will be failed if the authentication method is not configured

Command Mode

Global configuration mode

Usage Guidelines

The default list or other defined lists created by the **command aaa authentication dot1x** will be quoted by dot1x application and thus the dot1x user will be authenticated.

The next authentication method will be adopted only when the former method is failed. Other authentication method will not be adopted if the former authentication method return is failed

dot1x Authentication Method

Keyword	Description
group name	Uses the server group for authentication
group radius	Uses tacacs for authentication
group tacacs+	Uses TACACS+ for authentication
local	Uses the local user name data base for authentication
local-case	Uses case-sensitive local username for authentication.
none	Uses no authentication.

Example

The following example shows how to create an authentication method list named "TEST". The authentication first tries to connect with TACACS+ server. If no result (either "success" or "failure") is acquired from the TACACS+ server group (no dead error returned from TACACS+ server), try another method: local. If the local method can't acquire accurate result either, the internet can be accessed without authentication. (Up to now the device's authentication methods including aaa system enable(line) and local can acquire an accurate result either success or failure. Therefore, the following command has no none method.)

aaa authentication dot1x TEST group tacacs+ local none

The following example shows how to create a same list but configured with default list. If no other list is designated, the list is available to all dot1x authentications.

aaa authentication dot1x default group tacacs+ local none

Related Command

None

66.4.2 aaa authentication enable default

Syntax

To enable AAA authentication to determine if a user can access the privileged command level, use the aaa authentication enable default global configuration command. Use the no form of this command to disable this authentication method

aaa authentication enable default method1 [method2...]

no aaa authentication enable default

Parameter

method	At least one of the keywords described in "enable authentication method"

Default

The authentication method is not configured. The authentication process returns successfully if the user is the console port. Otherwise, the authentication process fails

Command Mode

Global configuration mode

Usage Guidelines

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 1. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line

Table 0- 1 aaa authentication enable default Methods

Keyword	Description
enable	Uses the enable password for authentication
group name	Uses the server group for authentication
group radius	Uses RADIUS for authentication
group tacacs+	Uses tacacs+ for authentication
line	Uses the line password for authentication

none	Uses no authentication

Example

The following example shows how to create an authentication method list named "TEST". The authentication first tries to connect with TACACS+ server. If no result (either "success" or "failure") is acquired from the TACACS+ server group (no dead error returned from TACACS+ server), try another method: local. If the local method can't acquire accurate result either, the internet can be accessed without authentication. (Up to now the device's authentication methods including aaa system enable(line) and local can acquire an accurate result either success or failure. Therefore, the following command has no none method.)

aaa authentication enable default group tacacs+ enable none

Related Command

enable password

66.4.3 aaa authentication login

Syntax

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the no form of this command

aaa authentication login {**default** | list-name} method1 [method2...]

no aaa authentication login {**default** | list-name}

Parameter

Parameter	Description
Default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in
list-name	Character string used to name the list of authentication methods activated when a user logs in
method	At least one of the keywords described in "login authentication method"

Default

The authentication method is not configured. The authentication process returns successfully if the user is the console port. Otherwise, the authentication process fails

Command Mode

Global configuration mode

Usage Guidelines

The default and optional list names that you create with the **aaa authentication login** command are used with the login authentication command

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed

AAA authentication login Methods

Keyword	Description
enable	Uses the enable password for authentication
group name	Uses the server group for authentication
group radius	Uses RADIUS for authentication
group tacacs+	Uses tacacs+ for authentication
line	Uses the line password for authentication
local	Uses the local username database for authentication
localgroup	Uses the local strategy group user name database for authentication
local-case	Uses case-sensitive local username for authentication
none	Uses no authentication

Example

The following example creates an AAA authentication list called TEST. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication

aaa authentication login TEST group tacacs+ group radius none

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

aaa authentication login default group tacacs+ group radius none

Related Command

None

66.4.4 aaa group server

Syntax

To group different RADIUS server hosts into distinct lists and distinct methods, enter the aaa group server radius

command in global configuration mode. To remove a group server from the configuration list, enter the no form of this command

aaa group server {radius | tacacs+} group-name

no aaa group server {radius | tacacs+} group-name

Parameter

Parameter	Description
group-name	Character string used to name the group of servers

Default

No server group

Command Mode

Global configuration mode

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service. It can set 63 server groups at most

Example

The following example adds a radius server group named radius-group:

aaa group server radius radius-group

Related Command

server

66.4.5 server

Syntax

To add a server in the AAA server group, use the server command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the no form of this command

server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}] [**auth-port** *num*] [**acct-port** *num*] [**retransmit** *value*] [**timeout** *value*] [**privilege** *pri*]

To add a server in the radius server group, use the following command:

server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}]

no server A.B.C.D

Parameter

Parameter	Description
A.B.C.D	IP address of the server
X:X:X:X::X	IPv6 address of the server
key	key
password	the character string of the key
encryption-type	Encryption type, 0 means no encryption, 7 means encryption
encrypted-password	Encryption password character string corresponding to the encryption type
auth-port	authentication destination port
acct-port	account port
num	port number
retransmit value	Retransmit times, the default is twice
timeout value	Timeout for retransmit; the default is 3 seconds
privilege pri	Server priority; the default is 0

Default

No server

Command Mode

Server-group configuration

Usage Guidelines

You can set 63 server groups in maximum, 1 radius server chain table and 1 tacacs+ server chain table. The total of all radius server groups and server groups in the server chain tables is 64. The total of all tacacs+ server groups and server groups in the server chain tables is also 64

Example

The following example adds a server at 12.1.1.1 to the server group:

server 12.1.1.1

Related Command

aaa group server

66.4.6 debug aaa authentication

Syntax

To display information on authentication, authorization, and accounting (AAA) TACACS+ authentication, use the **debug aaa authentication** command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug aaa authentication

no debug aaa authentication

Parameter

None

Default

Disable debug information

Command Mode

EXEC mode

Usage Guidelines

Use this command to learn the methods of authentication being used and the results of these methods

Example

None

Related Command

None

66.4.7 enable password

Syntax

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove the password requirement, use the no form of this command

enable password { *password* | [*encryption-type*] *encrypted-password* } [**level** *number*]

no enable password [**level** *number*]

Parameter

Parameter	Description
password	Password users type to enter enable mode
encryption-type	Algorithm used to encrypt the password
encrypted-password	Encrypted password you enter, copied from another router configuration

level	Level for which the password applies
number	Number between 1 and 15 that specifies the privilege level for the user

Default

No password is defined

Command Mode

Global configuration mode

Usage Guidelines

There cannot have spaces in the password that the router configures. When using the enable password command, you cannot input space if you enter a clear text password. The length of the clear text password cannot exceed 32 characters

The default level Parameter is 15 without inputting the level Parameter. If a privilege level is not configured password, then no authentication is performed when a user entering this privilege level

Our system only supports three types of encryption. The encryption type is 0, 2 and 7 respectively. Parameter 0 indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 2 indicates using sha256 encryption; Parameter 7 indicates a self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encrypted text password can be copied from the configuration file of other device

Example

The following example adds password clever for the privilege level 10, uses encryption-type 0, that is, the clear text password:

enable password 0 clever level 10

The following example adds password Oscar for the default privilege (15), uses encryption-type 2, that is, sha256 encryption method, the plaintext password:

enable password 2 Oscar

The following example adds password Oscar for the default privilege (15), uses encryption-type 7, that is, the encrypted text password:

enable password 7 074A05190326

Assuming the encrypted text password of Oscar is 074A05190326, which is obtained from the configuration file of other router

Related Command

aaa authentication enable default

service password-encryption

66.4.8 enable(enter)

Syntax

To enter the EXEC mode when logging in the system, run **enable(enter)** command.

enable(enter) <1-15>

Parameter

Parameter	Description
<1-15>	To be obtained privilege priority

Default

Do not enter the privileged mode

Command Mode

User mode

Usage Guidelines

None

Example

>enable(The user is 15 by default.)

Password: (To authenticate by entering the password)

#

#exi

>enable 1(To be obtained privilege priority is 1.)

Password:(Enter password to authenticate.)

#

Related Command

aaa authentication enable default

enable password

66.4.9 service password-encryption

Syntax

To encrypt passwords, use the service password-encryption command in global configuration mode. To restore the default, use the no form of this command

service password-encryption

no service password-encryption

Parameter

None

Default

No encryption

Command Mode

Global configuration mode

Usage Guidelines

Currently in the realization of our router system, this command is related to username password, enable password and password. If this command is not configured on the router (namely default state), and the system uses the clear text storage method in the above three commands, then the configured clear text of the password can be displayed in the show running-config command. If this command is configured on the router, then the configured password of the above three commands will be encrypted, then the configured clear text of the password cannot be displayed in the show running-config command, even using the no service password-encryption cannot restore the clear text of the password. Please make sure of the configured password before using this command for encryption. The no service password-encryption command only has effect on the password configured by the service password-encryption command

Example

Use the following command to encrypt for the configured clear text password and also to encrypt for the clear text password that configured after using this command

switch_config#service password-encryption

Related Command

username username **password**

enable password

password (the configuration command in vty which can be used for line authentication.)

66.5 aaa authorization

Syntax

The global configuration command "aaa authorization" is used for setting the parameter to limit the authority of the user's access to network. The "no" format of the command can be used for closing the authorization of some function

aaa authorization {{commands *<0-15>***} | network** | **exec}** {**default** | *list-name*} *method1* [*method2...*]

no aaa authorization {{commands *<0-15>***} | network** | **exec}** {**default** | *list-name*}

aaa authorization config-commands

no aaa authorization config-commands

Parameter

Parameter	Description
commands	EXEC (shell) command authorization
<0-15>	Priority of the to be authorized command
network	The authorization of network type service, such as PPP, SLIP
exec	It is applicable to the attribute related to the user EXEC terminal dialogue. It determines whether the EXEC shell program can be enabled when users register the system or authorize users the priority of entering EXEC shell
default	Default authorization methods list
list-name	The character string used for naming authentication methods list
method	One of the keywords listed in the form below
config-commands	Configuration mode command service

Default

When the user requests for authorization and the authorization methods list required for use is not designated on the corresponding line or the interface, the default authorization methods list will be used. If default methods list is defined, no authorization will take place

Command Mode

Global configuration mode

Usage Guidelines

The command “aaa authorization” is used for enabling the authorization, creating authorization methods list and defining the authorization method that can be used when the user accesses to the designated functions. The authorization methods list defines the method for authorization implementation and sequence for executing these authorization methods. The methods list is only a simple naming list describing the authorization method for inquiry on the sequence (such as RADIUS and TACACS+). The methods list can designate one or multiple security protocols used for authorization. So it is able to guarantee a backup method in case all the above listed authorization methods fail. Under general condition, the listed first method is used at first in an attempt to authorize the user the authority to access to the designated network service. If the method does not work, the next method in the list shall be selected. The process shall be continued till the successful feedback of authorization results by using some authorization method or all the defined methods are used up

Keyword of AAA Authorization

Keyword	Description
group name	Uses group name for authorization
group radius	Uses radius for authorization

group tacacs+	Uses tacacs+ for authorization
if-authenticated	Uses if-authenticated for authorization
local	Uses the local database for authorization
none	Uses no authentication

Once the authorization methods list is defined, the methods list shall be used on the designated line or interface before the defined method is executed. As a part of the authorization process, the authorization command sends a series of request packets of AV pairs to the program of RADIUS or TACACS＋server. The server is likely to execute one of the following actions:

The request is accepted completely

The request is accepted and the attribute is added to limit the authority of user service

Request is refused and authorization fails

Example

The following Example defines the network authorization methods list named “have a try”. The methods list designates RADIUS authorization method used on the serial line employing PPP. If RADIUS server makes no response, the local network authorization is executed

aaa authorization exec have_a_try radius local

Related Command

aaa authentication

aaa accounting

66.6 debug aaa authorization

Syntax

To track the authorization process, use debug **aaa authorization** command. To return to the default setting, use the no form of this command

debug aaa authorization

no debug aaa authorization

Parameter

None

Default

Disable debug information

Command Mode

EXEC mode

Usage Guidelines

The command is used to track the authorization process of each user, so that the reason of failure can be found

Example

None

Related command

None

66.7 aaa accounting

Syntax

To execute AAA accounting onto required services on the basis of accounting or security, run **aaa accounting** in global mode. You can run **no aaa accounting** to disable the accounting function

aaa accounting {{**commands** *<0-15>*} **| network** | **exec** | **connection**} {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** {*groupname* /**radius | tacacs+**}} | **none** }

no aaa accounting { **network** | **exec** | **connection**} {**default** | *list-name*}

Parameter

Parameter	Description
commands	EXEC (shell) command authorization
<0-15>	Priority of the to be authorized command
network	The authorization of network type service, such as PPP, SLIP
exec	It is applicable to the attribute related to the user EXEC terminal dialogue. It determines
connection	Provides information about all egress connections from related router. Currently, only the H323 session is supported
default	Default authorization methods list
list-name	The character string used for naming authentication methods list
Start-stop	Start and stop accounting
Stop-only	Stop accounting
None	No accounting
group groupname	Uses the server group for accounting
group radius	Uses RADIUS for accounting
group tacacs+	Uses TACACS+ for accounting

Default

If the user requires accounting but he does not designate the accounting method list on the corresponding path or interface, the default accounting method list will be applied. If the default method list is not defined, the accounting will not be executed

Command Mode

Global configuration mode

Usage Guidelines

You can use the **aaa accounting** command to enable the accounting function, create the accounting method list and define the applied accounting method when user sends the accounting record. The accounting method list defines the accounting execution method and the order to execute these accounting methods. The method list is just a simple naming list, describing the accounting method (RADIUS or TACACS+). The method list can designate one or multiple accounting security protocols. Hence, it secures a standby method if all previous accounting methods fail

Related Command

aaa authentication

aaa accounting

66.8 aaa accounting update

Syntax

To periodically transmit temporary accounting records to the accounting server, run **aaa accounting update**. You can run **no aaa accounting update** to disable temporary accounting records.

aaa accounting update { **newinfo** | **periodic** *number*}

no aaa accounting update { **newinfo** | **periodic**}

Parameter

Parameter	Description
update	Activates the router to transmit temporary accounting records
newinfo	Transmits temporary accounting records to the accounting server when new accounting information need be reported
periodic	Periodically transmits temporary accounting records. The period is defined by the **number** Parameter
number	A Parameter to define the period for temporary accounting record transmission

Default

Temporary accounting activity does not occur

Command Mode

Global configuration mode

Usage Guidelines

The function works with the support of the application end. Therefore, it is inapplicable at present

Related Command

aaa accounting

66.9 aaa accounting suppress null-username

Syntax

To stop generating accounting records for those non-user sessions, run aaa accounting suppress null-username in global mode. You can run no aaa accounting suppress null-username to resume the default configuration.

aaa accounting suppress null-username

no aaa accounting suppress null-username

Parameter

None

Default

The accounting records will be generated for all sessions, no matter the sessions have username or not

Command Mode

Global configuration mode

Usage Guidelines

None

Related Command

aaa accounting

66.10 debug aaa accounting

Syntax

To track the accounting process, use debug aaa accounting command. To return to the default setting, use the no form of this command

debug aaa accounting

no debug aaa accounting

Parameter

None

Default

Disable debug information

Command Mode

EXEC mode

Usage Guidelines

The command is used to track the accounting process of each user, so that the reason of failure can be found

Example

None

Related Command

None

66.11 localauthen

Syntax

To configure the local authentication policy, run **localauthen** command in the global configuration mode. To return to the default setting, use the no form of this command.

localauthen *WORD*

no localauthen *WORD*

Parameter

Parameter	Parameter Description
WORD	name of local authentication policy

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the local authentication policy configuration, use localauthen WORD command. Use the following command to configure the local authentication policy:

The maximum tries with a certain time:

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

Parameter	Parameter Description
max-tries	the maximum tries
<1-9>	The maximum tries ranges from 1 to 9.
try-duration	The duration for login trial.
1d2h3m4s	The format of day, hour, minute and second.

Related Command

login max-tries

localgroup

local authen-group

username

66.12 localauthor

Syntax

To configure the local authorization policy, run localauthor command in the global configuration mode. To return to the default setting, use the no form of this command

localauthor *WORD*

no localauthor *WORD*

Parameter

Parameter	Parameter Description
WORD	Name of the local authorization policy

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the local authorization policy configuration, use **localauthen WORD** command. Use the following command to configure the local authorization policy:

To authorize the priority for the login user

exec privilege {**default | console | ssh | telnet**} *<1-15>*

Parameter	Parameter Description
default	The default priority (when the concrete login method is not configured, authorize by the priority.)
console	The authorization priority of the login user in the console port.
ssh	The authorization priority of the ssh login user
telnet	The authorization priority of the telnet login user
<1-15>	Priority

Related Command

exec privilege

localgroup

local author-group

username

66.13 localpass

Syntax

To configure the local password policy, use **localpass** command. To return to the default setting, use the no form of this command

localpass *WORD*

no localpass *WORD*

Parameter

Parameter	Parameter Description
WORD	Name of local password policy

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the localpass WORD policy configuration, use localpass WORD command. Use the following command to configure the local password policy:

1.The password and username is different

- **non-user**

2.History password check (It is different with the history password when modifying the user password)

- **non-history**

3.Designate the password content

- **element [number] [lower-letter] [upper-letter] [special-character]**

Parameter	Parameter Description
number	It must include numbers
lower-letter	It must include the lower letter
upper-letter	It must include the upper letter
special-character	It must include the special character

1.The minimum length of the password:

- min-length <1-127>

Parameter	Parameter Description
<1-127>	The minimum length (The range is 1-127)

2.The password validity:

- **validity** *1d2h3m4s*

Parameter	Parameter Description
1d2h3m4s	The format of day, hour, minute and second.

Related Command

non-use

non-history

element

min-length

validity

localgroup

local pass-group

username

66.14 localgroup

Syntax

To configure the local group, run **localgroup** command in the global configuration mode. To return to the default setting, use the no form of this command

localgroup *WORD*

no localgroup *WORD*

Parameter

Parameter	Parameter Description
WORD	Name of the local policy group

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the localgroup WORD policy configuration, use localpass WORD command. Use the following command to configure the local password policy:

- local authen-group
- local author-group
- local pass-group

- local user
- username

Related Commands

local authen-group

local author-group

local pass-group

local user

username

localgroup

local author-group

66.15 local authen-group

Syntax

To configure the local authentication group, run local authen-group command. The local authentication group is by default in the global configuration mode. To return to the default setting, use the no form of this command

local authen-group *WORD*

no local authen-group

Parameter

Parameter	Parameter Description
WORD	Name of local authentication group

Default

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related commands

localauthen

localgroup

local authen-group

66.16 local author-group

Syntax

To configure the local authorization group, use the local author-group command. The local authorization group is by default in the global configuration mode. To return to the default setting, use the no form of this command

local author-group *WORD*

no local author-group

Parameter

Parameter	Parameter Description
WORD	Name of the local authorization group

Default

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localauthor

localgroup

local author-group

66.17 local pass-group

Syntax

To configure the local password group, use the local pass-group command. The local pass-group is by default in the global configuration mode. To return to the default setting, use the no form of this command

local pass-group *WORD*

no local pass-group

Parameter

Parameter	Parameter Description
WORD	Name of the local password group

Default

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localpass

localgroup

local pass-group

66.18 local user

Syntax

To configure the maximum connections and freeze users of the account configured in the local group, run **local user** command. The local user group is by default in the global configuration mode. To return to the default setting, use the no form of this command.

local user {maxlinks *<1-255>***} | { freeze** *WORD***}**

no local user {maxlinks | { **freeze** *WORD* }**}**

Parameter

Parameter	Parameter Description
maxlinks	Limit the number of login users simultaneously for one user name
<1-255>	amount (range from 1-255)
freeze	freeze users
WORD	user name

Default

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related command

localgroup

66.19 username

Syntax

To add users in the local user database for local authentication and authorization, run the following command. The username is by default in the global configuration mode. To return to the default setting, use the no form of this command

username *username* [**password** *password* | {**encryption-type** *encrypted-password*}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**autocommand** *command*] [**bind-ip** *A.B.C.D*] [**bind-mac** *H:H:H:H:H:H*] [**bind-pool** *WORD*] [**bind-port** *port*][**callback-dialstring** *string*] [**callback-line** *line*] [**callback-rotary** *rotary*] [**nocallback-verify**] [**nohangup**] [**noescape**]

no username *username*

Parameter

Parameter	Parameter Description
username	user name character string
password	username password
password	Plain text of the password character string
encryption-type	Type of password encryption
encrypted-password	Cipher text of the password which corresponds to the limited encryption type
maxlinks	Links established by the account (the number of simultaneous login users of one user name)
number	the number of links
authen-group	Designate local authen-group
WORD	Name of local authen-group
author-group	Designate local author-group
WORD	Name of local author-group

pass-group	Designate local pass-group
WORD	Name of local pass-group
autocommand	Auto run the designated command after the user logs in. The auto command must be used at the end of the command line.
command	Auto run the command character string.
	Non-supported options
bind-ip	binding IP address (non-supported)
A.B.C.D	IP address
bind-mac	Binding user mac address (non-supported)
H:H:H:H:H:H	ARP recorded 48 byte hardware address
bind-pool	Binding user address pool (non-supported)
WORD	Address pool name
bind-port	Binding user port (non-supported)
port	Port
callback-dialstring	Call back telephone number (non-supported)
string	Telephone number character string;
callback-line	The line used in call back (non-supported)
line	ine number
callback-rotary	Call back rotary configuration (non-supported)
rotary	Rotary number
nocallback-verify：	No callback verification (non-supported)
nohangup	No hangup after the user logs in and auto run the command (non-supported)
noescape	No escape character after the user logs in (non-supported)

Default

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

The password is empty character string when there is no password parameter

User-maxlinks limit the established number of sessions simultaneously in one account. The session will not be count in if it is not authenticated by the local auth-group. To check the basic information of teach online user, run show aaa users command

Our switch system only supports three types of encryption. The encryption type is 0, 2 and 7 respectively. Parameter 0 indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 2 indicates using sha256 encryption; Parameter 7 indicates a self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encrypted text password can be copied from the configuration file of other switches

Example

The following example shows how to add local users whose user name is someone and whose password is someother:

username someone password someother

The following example shows how to add local users whose user name is someone and whose password is someother:

username someone password 2 someone

The following example shows how to add the local user whose name is Oscar and whose password is Joan. The adopted encryption-type is 7. Enter the password ciphertext:

enable password 7 1105718265

Suppose that the cipher text of Joan is 1105718265, the value of the cipher text is obtained from the configuration files of other routers

Related command

aaa authentication login

66.20 show local-users

Syntax

To show the overview of all local AAA account, run show local-users command

show local-users

Parameter

None

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to show all AAA accounts which include Local group default, links, pw_present, login_tries, login_try_time and freezing_cause

Example

#show local-users

Local group default:

username	links	pw_present	login_tries	login_try_time	freezing_cause
admin	1	0s	0	0s	
aaa	0	0s	0	0s	

Domain	Description
Local group default:	local group
links	Links used by the account (It is how many users are using.)
pw_present	Password presence time (configure the valid password period)
login_tries	Password matching failure times (set the max login tries, 0 means no setting.)
login_try_time	Timeout of password matching failure (se the max login tries, 0 means no setting.)
freezing_cause	Reason of account freezing

Related command

username

66.21 show aaa users

Syntax

To show the overview of all online AAA users, run show aaa users command

show aaa users

Parameter

None

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command can be used to show information of all online users such as port, username, service type (service), online duration (time) and IP address (peer_address)

Example

#show aaa users

Port User Service Duration Peer Address

==========

console 0 zjlexec 04:14:03 unknown

vty 0aaa exec00:12:24 172.16.20.120

Domain	Description
Port	ID of the interface where user lies, or index number of VTY
User	Character string of username
Service	Service applied by the user
Duration	Online duration time of the user
Peer Address	IP address of the remote host where the user lies

Related command

username

Chapter 67 RADIUS Configuration Commands

67.1 debug radius

Syntax

To display information associated with RADIUS, use the debug radius command in

EXEC mode. To disable debugging output, use the no form of this command

debug radius {*event*|*packet*}

no debug radius {*event*|*packet*}

Parameter

Parameter	Description
event	Displays radius event
packet	Displays radius packet

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command can be used to debug network system to locate the authentication failure reason

Example

The following example debugs RADIUS event:

debug radius event

67.2 ip radius source-interface

Syntax

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the ip radius source-interface command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

ip radius source-interface *interface-name*

no ip radius source-interface

Parameter

Parameter	Description
interface-name	Name of the interface that RADIUS uses for all of its outgoing packets

Default

No default behavior or values

Command Mode

Global configuration mode

Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses

This command is especially useful in cases where the router has many subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address

The specified subinterface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the subinterface to the up state

Example

The following example shows how to configure RADIUS to use the IP address of vlan 1 for all outgoing RADIUS packets:

ip radius source-interface vlan 1

Related Command

ip tacacs source-interface

67.3 radius-server attribute

Syntax

To transmit some attributes in radius AAA, run the following command. To return to the default setting, use the no form of this command

radius-server attribute {4 | 32 | 95}

no radius-server attribute {4 | 32 | 95}

Parameter

Parameter	Parameter Description
4	Transmit the value of attribute 4 (NAS ip address) after the parameter in dealing with the radius.
32	Designate the transmission attribute 32 (NAS identifier) in radius authentication and accounting according to the command after the parameter
95	Designate the transmission attribute 95 (NAS ipv6 address) in radius authentication and accounting according to the command after the parameter

Default

None

Command Mode

Global configuration mode

Usage Guidelines

Use radius-server attribute command to designate a certain attribute in dealing with radius.

Use radius-server attribute 4 (NAS IP address) and designate transmission in RADIUS packet

Designate the transmission attribute 32 (NAS identifier) in radius authentication and accounting according to the command after the parameter

Designate the transmission attribute 95 (NAS ipv6 address) in radius authentication and accounting according to the command after the parameter

Example

radius-server attribute 4 X.X.X.X transmits radius attribute 4 in RADIUS packet and use X.X.X.X as the attribute value

radius-server attribute 32 in-access-req transmits NAS identifier in authentication request

radius-server attribute 32 in-account-req transmits NAS identifier in accounting request

radius-server attribute 32 identifier configures NAS identifier

radius-server attribute 95 X:X:X:X::X transmits radius attribute 95 in RADIUS packet and use X:X:X:X::X as the attribute value

Related Command

None

67.4 radius-server challenge-noecho

Syntax

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the radius-server challenge-noecho command in global configuration mode. To return to the default condition, use the no form of this command

radius-server challenge-noecho

no radius-server challenge-noecho

Parameter

None

Default

All user responses to Access-Challenge packets are echoed to the screen

Command Mode

Global configuration mode

Usage Guidelines

None

Example

radius-server challenge-noecho

67.5 radius-server deadtime

Syntax

To improve RADIUS response times when some servers might be unavailable and cause the unavailable servers to be skipped immediately, use the radius-server deadtime command in global configuration mode. To set dead-time to 0, use the no form of this command.

radius-server deadtime minutes

no radius-server deadtime

Parameter

Parameter	Description
minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours)

Default

Dead time is set to 0

Command Mode

Global configuration mode

Usage Guidelines

Use this command to cause the software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the duration of minutes or unless there are no servers not marked "dead."

Example

The following example specifies five minutes deadtime for RADIUS servers that fail to respond to authentication requests:

radius-server deadtime 5

Related Command

radius-server host

radius-server retransmit

radius-server timeout

67.6 radius-server directed-resquest

Syntax

To designate RADIUS server with the format of '@server', run radius-server directed-resquest command in the global configuration mode. To return to the default setting, use the no form of this command.

radius-server directed-resquest [restricted]

no radius-server directed-resquest [restricted]

Parameter

Parameter	Parameter description
restricted	Only enable the user to designate RADIUS server with the format of '@server'

Default

It doesn't support to designate RADIUS server with the format of '@server'

Command Mode

Global configuration mode

Usage Guidelines

None

Example

radius-server directed-resquest

Related Command

None

67.7 radius-server host

Syntax

To specify a RADIUS server host, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

radius-server host *ip-address|ipv6-address* [*auth-port port-number1*] [acct-port *port-number2*]

no radius-server host ip-address*/ipv6-address*

Parameter

Parameter	Description
ip-address	IP address of the RADIUS server host
ipv6-address	IPv6 address of the RADIUS server host
auth-port	(Optional) Specifies the UDP destination port for authentication requests
port-number1	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0
acct-port	(Optional) Specifies the UDP destination port for accounting requests
port-number2	(Optional) Specifies the UDP destination port for accounting requests; the host is not used for accounting if set to 0

Default

No RADIUS host is specified

Command Mode

Global configuration mode

Usage Guidelines

You can use multiple radius-server host commands to specify multiple hosts. The software searches for hosts in the order in which you specify them

Example

The following example specifies host 1.1.1.1 as the RADIUS server and uses default ports for both accounting and authentication

radius-server host 1.1.1.1

The following example specifies port 12 as the destination port for authentication requests and port 16 as the destination port for accounting requests on the RADIUS host named host1:

radius-server host 1.2.1.2 auth-port 12 acct-port 16

Related Command

aaa authentication

radius-server key

tacacs server

username

67.8 radius-server key

Syntax

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the radius-server key command in global configuration mode. To disable the key, use the no form of this command.

radius-server key *string* | {encryption-type encrypted-password}

no radius-server key

Parameter

Parameter	Description
string	Spedifies the encrypted key. This encrypted key must match the encrypted key that RADIUS server uses
encryption-type	encryption type, 0 means no encryption, and 7 means encryption
encrypted-password	The ciphertext of the password corresponding to the encryption type limited by "encryption-type"

Default

The encrypted key is the empty character string

Command Mode

Global configuration mode

Usage Guidelines

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, and all white spaces cannot be included in the encrypted key

Example

The following example sets the encryption key to " firstime ":

radius-server key firstime

Related Command

radius-server host

tacacs server

username

67.9 radius-server optional-passwords

Syntax

To specify that the first RADIUS request to a RADIUS server be made without password verification, use the radius-server optional-passwords command in global configuration mode. To restore the default, use the no form of this command

radius-server optional-passwords

no radius-server optional-passwords

Parameter

This command has no Parameters or keywords

Default

Disabled

Command Mode

Global configuration mode

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature

Example

The following example configures the first login to not require RADIUS verification:

radius-server optional-passwords

Related Command

radius-server host

67.10 radius-server retransmit

Syntax

To specify the number of times the software searches the list of RADIUS server hosts before giving up, use the radius-server retransmit command in global configuration mode. To disable retransmission, use the no form of this command

radius-server retransmit *retries*

no radius-server retransmit

Parameter

Parameter	Description
retries	Maximum number of retransmission attempts. The default is 2 attempts.

Default

2 attempts

Command Mode

Global configuration mode

Usage Guidelines

This command is generally used with the radius-server timeout command, indicating the interval for which a router waits for a server host to reply before timing out and the times of retry after timing out

Example

The following example specifies a retransmit counter value of five times:

radius-server retransmit 5

Related Command

radius-server timeout

67.11 radius-server timeout

Syntax

To set the interval for which a router waits for a server host to reply, use the radius-server timeout command in global configuration mode. To restore the default, use the no form of this command

radius-server timeout *seconds*

no radius-server timeout

Parameter

Parameter	Description
seconds	Number that specifies the timeout interval, in seconds. The default is 3 seconds

Default

3 seconds

Command Mode

Global configuration mode

Usage Guidelines

This command is generally used with the radius-server retransmit command

Example

Use this command to set the number of seconds a router waits for a server host to reply before timing out

radius-server timeout 10

Related Command

None

67.12 radius-server vsa send

Syntax

To configure the network access server to recognize and use vendor-specific attributes, use the radius-server vsa send command. To restore the default, use the no form of this command

radius-server vsa send [**authentication**]

no radius-server vsa send [**authentication**]

Parameter

Parameter	Description
authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

Default

Disabled

Command Mode

Global configuration mode

Usage Guidelines

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The radius-server vsa send command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the accounting keyword with the radius-server vsa send command to limit the set of recognized vendor-specific attributes to just accounting attributes. Use the authentication keyword with the radius-server vsa send command to limit the set of recognized vendor-specific attributes to just authentication attributes

Example

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

radius-server vsa send authentication

Related Command

radius-server host

67.13 radius-server acct-on

Relevant configuration about accounting function

[no] radius-server acct-on enable

Open/close radius accounting function

[no] radius-server acct-on retransmit <1-15>

Set the time of radius accounting retransmit, the default is 3times

Parameter

Parameter	Description
Retransmit	Times of radius accounting retransmit

Default

Close accounting function, the retransmit is 3 times

Command mode

Global configuration mode

Usage Guidelines

None

Example

The following example configures the switch. Open the accounting function, set the retransmit times as 5:

radius-server acct-on enable

radius-server acct-on retransmit 5

Related Command

None

Chapter 68 TACACS+ Commands

68.1 debug tacacs

Syntax

The command "debug tacacs" can be used for tracing TACACS+protocol event or checking the packets received or sent. The "no" format of the command can be used for canceling the trace.

debug tacacs {**event** | **packet**}

no debug tacacs {**event** | **packet**}

Parameter

Parameter	Description
event	**Tracing** TACACS+ event
packet	**Tracing** TACACS+ packet

Default

Disable debug information

Command Mode

EXEC mode

Usage Guidelines

The command is only used for the debugging of the network to find out the cause of failure of AAA service

Example

The following example will open the event trace of TACACS+

debug tacacs event

Related Command

None

68.2 p tacacs source-interface

Syntax

The global configuration command "ip tacacs source-interface" is used for applying IP

address of the designated interface to all the TACACS＋ packets. The "no" format of

the command cancel the using of the IP address.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Parameter

Parameter	Description
subinterface-name	Interface name corresponding to the source IP address of all TACACS+ packets.

Default

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to set source IP address for all TACACS＋packets by designating the source interface. So long as the interface is under "up" state, all TACACS+ packets will use IP address of the interface as the source address, thus ensuring that TACACS+ packet of each router will have the same source IP address. So TACACS＋server will not need to maintain the address list containing the IP address. That is to say, in order to ensure all TACACS＋packets coming from the specific router to have the same source IP address, the command will work when the router has many interfaces

The designated interface shall have the IP address linked to the interface. If the designated interface has no IP address or is under a "down" state, the default value will be restored, namely the source IP address shall be determined on the real condition. In order to avoid the case, the IP address shall be added to the interface and the interface shall be ensured under the "up" state

Example

The following Example will use IP address of the interface s1/0 as source IP address of all TACACS+ packets

ip tacacs source-interface vlan1

Related Command

ip radius source-interface

68.3 tacacs-server host

Syntax

The command "tacacs-server host" can be used for designating TACACS+ server, run tacacs-server host command. To return to the default setting, use the no form of this command.

tacacs-server host *ip-address* [**single-connect**|**multi-connect**] [**port** *integer1*] [**timeout** *integer2*] [**key** *string*]

no tacacs-serve *ip-address*

Parameter

Parameter	Parameter Description

ip-address	IP address of the server
single-connect	(optional) Maintain a single open TCP connection from AAA/TACACS+ server
multi-connect	(optional) Maintain multiple TCP connections from AAA/TACACS+ server
port	(optional) Set port number. The option covers up the default port number 49
integer1	(optional) The port number of the server. The effective port number ranges from 1 to 65536
timeout	(optional) Set timeout value of the server. It covers up the global timeout value for the server by tacacs command
integer2	(optional) Set timeout value by seconds
key	(optional) Set authentication and encryption key. The key must be match with the key of TACACS+ server program. The key covers up the server key of global tacacs key
string	(optional) Set encryption key character string

Default

No TACACS+ server is set

Command Mode

Global Configuration Mode

Usage Guidelines

Use tacacs-server commands to set multiple hosts and explore the host in order. As some parameters of tacacs-server host command cover up configurations tacacs-server timeout and tacacs-server key commands set in global configuration mode. Therefore, the command can configure the communication attribute of each TACACS+ server

Example

The following example shows how to negotiate the router and TACACS+ server whose IP address is 1.1.1.1 (for AAA) and set the TCP service port of the server as 51. The timeout value is 3 seconds and the encryption key is a_secret

tacacs -server host 1.1.1.1 single-connection port 51 timeout 3 key a_secret

68.4 tacacs-server key

Syntax

To set the encryption keys between the router and TACACS+ server, run tacacs-server key command in the global configuration mode. To return to the default setting, use the no form of this command.

tacacs-server key

no tacacs-server key y

Parameter

Parameter	Parameter Description
key	It is used for setting the encryption key. The encryption key must be match with the key of TACACS+ server program

Command Mode

Global Configuration Mode

Usage Guidelines

The encryption key must be set by tacacs-server key command before running TACACS+ protocol. The encryption key must be match with the key of TACACS+ service program. All spaces must be avoided

Example

The following example shows how to set the encryption key as testkey:

tacacs-server key testkey

68.5 tacacs-server timeout

Syntax

The command "tacacs timeout" can be used to set the length of timeout for TACACS+ to wait for the response from some server. The "no" format of the command can be used for restoring default value.

tacacs timeout *seconds*

no tacacs timeout

Parameter

Parameter	Description
seconds	The value of timeout calculated on second (between 1 to 600). The default value is 5 seconds.

Default

5 seconds

Command Mode

Global configuration mode

Usage Guidelines

If some server sets its own timeout value of waiting through the parameter in the command "tacacs server", the value will cover the global timeout value set by this command

Example

The Example below changes the value of timeout timer as 10 seconds

tacacs-server timeout 10

Chapter 69 SGNP Configuration Commands

69.1 bvss sgnp neighbour-timeout

Syntax

To configure the timeout of SGNP neighbors, run the following command. To restore the default value, run the no form of the command

bvss sgnp neighbour-timeout *value*

no bvss sgnp neighbour-timeout

Parameters

Parameters	Description
value	The timeout of SGNP neighbors, range: 3-10 seconds

Default Value

3 seconds.

Usage Guidelines

None

Example

The following example shows how to configure the timeout of SGNP neighbors to 10 seconds:

Switch_config#bvss

Switch_config_bvss#bvss sgnp neighbor-timeout 10

69.2 show bvss sgnp

Syntax

To show the configuration and state information of SGNP, run the following command

show bvss sgnp

Parameters

None

Default Value

None

Usage Guidelines

None

Example

None

Chapter 70 STP Configuration Commands

70.1 SSTP Configuration Commands

70.1.1 spanning-tree

Syntax

spanning-tree

no spanning-tree

To enable the default STP mode, run **spanning-tree**; to disable the STP, run **no spanning-tree**

Enable or disable STP in interface configuration mode

Parameter

None

Default

Enable RSTP mode by default

Usage guidelines

None

Command Mode

Global configuration mode

Physical port or aggression port configuration mode

Example

None

70.1.2 spanning-tree mode sstp

Syntax

spanning-tree mode sstp

no spanning-tree mode

To switch between RSTP and SSTP modes, use the **spanning-tree mode** command. To return to the default settings, use the no form of this command

Parameter

None

Default

RSTP

Usage guidelines

None

Command Mode

Global configuration

Example

The following command shows how to enable SSTP mode:

Switch_config# spanning-tree mode sstp

Switch_config#

70.1.3 spanning-tree sstp priority

Syntax

To set the sstp bridge priority, use the spanning-tree sstp priority command. To return to the default settings, use the no form of this command

spanning-tree sstp priority *value*

no spanning-tree sstp priority

Parameter

Parameter	Description
value	Value is from 0 to 61440

Default

32768

Usage Guidelines

When setting the priority value, you can make the node as the root of the spanning tree. The configuration value takes 4096 as a step and its value is the multiple of 4096. The configurable values are 0, 4096, 8192, 3*4096, 4*4096, …and 15*4096

Command mode

Global configuration

Example

This example shows how to set the SSTP priority to 4096:

Switch(config)# spanning-tree sstp priority 4096

Switch(config)#

70.1.4 spanning-tree sstp hello-time

Syntax

To set the hello-time delay timer, use the spanning-tree sstp hello-time command. To return to the default settings, use the no form of this command

spanning-tree sstp hello-time *time*

no spanning-tree sstp hello-time

Parameter

Parameter	Description
time	Number of seconds to set the hello-time delay timer; valid values are from 1 to 10 seconds

Default

2s

Usage Guidelines

The hello-time configured by the local OLT is valid only when the local OLT is the root OLT

Command mode

Global configuration

Example

The following example sets the SSTP hello-time to 8 seconds:

Switch(config)# spanning-tree sstp hello-time 8

Switch(config)#

70.1.5 spanning-tree sstp max-age

Syntax

To set the SSTP max-age timer, use the spanning-tree sstp max-age command. To return to the default settings, use the no form of this command

spanning-tree sstp max-age *time*

no spanning-tree sstp max-age

Parameter

Parameter	Description
seconds	Number of seconds to set the max-age timer; valid values are from 6 to 40 seconds

Default

20s

Usage Guidelines

None

Command mode

Global configuration

Example

This example shows how to set the max-age timer to 24 seconds：

Switch(config)# spanning-tree sstp max-age 24

Switch(config)#

70.1.6 spanning-tree sstp forward-time

Syntax

To set the forward-delay timer, use the spanning-tree sstp forward-time command in global configuration mode. To return to the default settings, use the no form of this command

spanning-tree sstp forward-time *time*

no spanning-tree sstp forward-time

Parameter

Parameter	Description
time	Number of seconds to set the forward-delay timer; valid values are from 4 to 30 seconds

Default

15 seconds

Usage Guidelines

None

Command mode

Global configuration

Example

The following example shows how to set forward delay timer to 20 seconds:

Switch_config# spanning-tree sstp forward-time 20

Switch_config#

70.1.7 spanning-tree sstp cost

Syntax

To set the path cost of the interface for SSTP calculations, use the spanning-tree sstp cost command in interface configuration mode. To return to the default value, use the no form of this command

spanning-tree sstp cost *value*

no spanning-tree sstp cost

Parameter

Parameter	Description
value	Path cost. Valid values are from 1 to 200000000

Default

10M Ethernet:100

100M Ethernet: 19

1000M Ethernet: 4

Usage Guidelines

None

Command mode

Interface configuration

Example

This example shows how to set a path cost value of 100 for the spanning tree VLAN associated with the interface G0/1:

Switch_config_g0/1#spanning-tree sstp cost 100

Switch_config_g0/1#

70.1.8 spanning-tree cost

Syntax

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the spanning-tree cost command in interface configuration mode. To return to the default value, use the no form of this command

spanning-tree cost *value*

no spanning-tree cost

Parameter

Parameter	Description
value	Path cost; valid values are from 1 to 200000000

Default

The default path cost is computed from the bandwidth setting of the interface

Usage Guidelines

The configuration result of this command is valid to all spanning-tree modes. In STP mode, the path cost of all VLAN spanning-trees on the interface will be updated. In MSTP mode, the path cost of all spanning-tree examples will be updated

But the configuration result of the command will not influence the independent configuration in various modes. For example, the OLT respectively configured with the spanning-tree sstp cost 100 and the spanning-tree cost 110 in SSTP mode, the port priority will be 100

Command mode

Interface configuration

Example

This example shows how to set a path cost value of 24 for the spanning tree VLAN associated with the interface g0/1:

Switch(config_f0/0)# spanning-tree cost 24

Switch_config_g0/1#

70.1.9 spanning-tree sstp port-priority

Syntax

To set the priority value in SSTP mode, use the spanning-tree sstp port-priority command. Use the no form of this command to restore the default value

spanning-tree sstp port-priority *value*

no spanning-tree sstp port-priority

Parameter

Parameter	Description
value	Port priority. Value is from 0 to 240

Default

128 (0x80)

Usage Guidelines

The port priority must be set in increments of 16 only

Command mode

Interface configuration

Example

The following example sets 32 as the priority value on interface g0/1:

Switch_config_g0/1# spanning-tree sstp port-priority 32

Switch_config_g0/1#

70.1.10 spanning-tree port-priority

Description

To prioritize an interface when two bridges compete for position as the root bridge, use the spanning-tree port-priority command. The priority you set breaks the tie. To return to the default value, use the no form of this command

spanning-tree port-priority *value*

no spanning-tree port-priority

Parameter

Parameter	Description
value	Port priority. Value is from 0 to 240. Step: 16

default

Port priority value is 128

Usage Guidelines

The configuration result of this command is valid to all spanning-tree modes. In STP mode, the priority of all VLAN spanning-trees on the interface will be updated. In MSTP mode, the priority of all spanning-tree examples will be updated

But the configuration result of the command will not influence the independent configuration in various modes. For example, the OLT respectively configured with the spanning-tree sstp port-priority 128 and the spanning-tree port-priority 48 in SSTP mode, the port priority will be 128

Command mode

Interface configuration

example

The following example shows how to set the priority value to g0/1:

Switch_config_g0/1#spanning-tree port-priority 16

Switch_config_g0/1#

70.1.11 show spanning-tree

Syntax

To display spanning-tree information for the specified spanning-tree instances, use the show spanning-tree command

show spanning-tree [**detail** | **interface** *intf-i*]

Parameter

Parameter	Description
intf-i	Interface name, for instance, G0/1

Default

None

Usage Guidelines

Show spanning-tree state

Command mode

EXEC/Global configuration/Interface configuration

Example

Switch_config#show spanning-tree

Spanning tree enabled protocol SSTP

SSTP

Root ID Priority 32768

Address 00E0.0FCC.F775

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address 00E0.0FCC.F775

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Pri.Nbr Type

---------- ---- --- --------- ------- --------------------------------

G0/1 Desg FWD 19 128.16 P2p

Switch_config#

70.1.12 spanning-tree management trap

Syntax

To enable STP Trap, run command **spanning-tree management trap** [**newroot** | **topologychange**]. To return to the default value, use the no form of this command

[no] spanning-tree management trap [**newroot** | **topologychange**]

Parameter

Parameter	Description
newroot	newRoot Trap type
topologychange	topologyChange Trap type

Default

STP Trap is not enabled

Usage guidelines

None

Command mode

Global configuration

Example

None

70.2 VLAN STP Configuration Commands

70.2.1 spanning-tree mode pvst

Syntax

spanning-tree mode pvst

no spanning-tree mode

To enable STP modes, use the **spanning-tree mode pvst** command. To disable all STP modes, use the no form of this command

Parameter

None

Default

RSTP mode

Usage guidelines

None

Example

The following command shows how to enable PVST in switch.

Switch_config# spanning-tree mode pvst

Switch_config#

70.2.2 spanning-tree vlan

Syntax

spanning-tree vlan *vlan-list*

no spanning-tree vlan *vlan-list*

To configure a STP instance for a specified VLAN, use **spanning-tree vlan** *vlan-list* command. To remove the specified spanning-tree vlan, use no form of the command

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15

Default

Switch can configure spanning-tree for a certain number of VLAN. In default mode, the exceeded VLAN will be prohibited

Usage guidelines

None

Command Mode

Global configuration mode

Example

The following command shows how to remove the spanning-tree of VLAN10, 11, 15-19, and configure the spanning-tree for VLAN 40-50:

Switch_config#no spanning-tree vlan 10,11,15-19

Switch_config#spanning-tree vlan 40-50

Switch_config#

70.2.3 spanning-tree vlan priority

Syntax

spanning-tree vlan *vlan-list* **priority** *value*

no spanning-tree vlan *vlan-list* **priority**

Use the command to configure the bridge priority value for the spanning-tree in specified VLAN

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15
value	Priority values, ranging from 0 to 61440, step: 4096

Default

In default mode, the bridge priority value of the spanning-tree VLAN is 32768 plus VLAN number

Usage guidelines

None

Command Mode

Global configuration mode

Example

The following command shows how to configure the bridge priority value of VLAN1-3, 5-10 to 4096:

Switch_config#spanning-tree vlan 1-3,5-10 priority 4096

Switch_config#

70.2.4 spanning-tree vlan forward-time

Syntax

spanning-tree vlan *vlan-list* **forward-time** *value*

no spanning-tree vlan *vlan-list* **forward-time**

To set the Forward DelayParameter of the specified spanning-tree vlan, use **spanning-tree vlan *vlan-list* forward-time *value*** command. To return to the default settings, use the no form of this command

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15
value	Forward-Delay value, ranging from 4s to 30s. The default value is 15s

Default

All VLAN Forward Delay is 15s

Usage guidelines

None

Command Mode

Global configuration mode

Example

The following command shows how to configure the Forward Delay of VLAN1-3, 5-10 to 19s:

Switch_config#spanning-tree vlan 1-3,5-10 forward-time 19

Switch_config#

70.2.5 spanning-tree vlan max-age

Syntax

spanning-tree vlan *vlan-list* **max-age** *value*

no spanning-tree vlan *vlan-list* **max-age**

To set the Max AgeParameter of the specified spanning-tree vlan, use **spanning-tree vlan *vlan-list* max-age *value*** command. To return to the default settings, use the no form of this command

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15
value	max-age value, ranging from 6s to 40s. Its default value is 20s

Default

All VLAN Max Age is 20s

Usage guidelines

None

Command Mode

Global configuration mode

Example

The following command shows how to configure the Max Age of VLAN1-3, 5-10 to 19s:

Switch_config#spanning-tree vlan 1-3,5-10 max-age 19

Switch_config#

70.2.6 spanning-tree vlan hello-time

Syntax

spanning-tree vlan *vlan-list* **hello-time** *value*

no spanning-tree vlan *vlan-list* **hello-time**

To set the hello-timeParameter of the specified spanning-tree vlan, use **spanning-tree vlan *vlan-list* hello-time *value*** command. To return to the default settings, use the no form of this command

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15
value	hello-time value, ranging from 1s to 10s. Its default value is 2s

Default

All VLAN Hello-Time is 2s

Usage guidelines

None

Command Mode

Global configuration mode

Example

The following command shows how to configure the Hello Time of VLAN1-3, 5-10 to 9s:

Switch_config#spanning-tree vlan 1-3,5-10 hello-time 9

Switch_config#

70.2.7 spanning-tree vlan cost

Syntax

spanning-tree vlan *vlan-list* **cost** *value*

no spanning-tree vlan *vlan-list* **cost**

To set the path cost of the interface for Spanning Tree Protocol (STP), use the **spanning-tree vlan** ***vlan-list*** **cost** ***value*** command. To return to the default value, use the no form of this command

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15
value	The path cost of the interface rangings from 1 to 200000000

Default

The path cost depends on the connection rate of the port

The path cost value of 10M Ethernet is 100

The path cost value of 100M Ethernet is 19

The path cost value of 1000M Ethernet is 1

Usage guidelines

None

Command Mode

Interface configuration mode

Example

The following command shows how to configure the path cost of VLAN1-3, 5-10 in the interface G0/1 to 100:

Switch_config_g0/1#spanning-tree vlan 1-3,5-10 cost 100

Switch_config_g0/1#

70.2.8 spanning-tree vlan port-priority

Syntax

spanning-tree vlan *vlan-list* **port-priority** *value*

no spanning-tree vlan *vlan-list* **port-priority**

To set the interface priority for Spanning Tree Protocol (STP), use the **spanning-tree vlan** ***vlan-list*** **port-priority** ***value*** command. To return to the default value, use the no form of this command

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15
value	Interface priority, ranging from 0 to 240, step: 16

Default

128

Usage guidelines

None

Command Mode

Interface configuration mode

Example

The following command shows how to configure the priority of VLAN1-3, 5-10 in the interface G0/1 to 32:

Switch_config_g0/1#spanning-tree vlan 1-3,5-10 port-priority 32

Switch_config_g0/1#

70.2.9 show spanning-tree vlan

Syntax

show spanning-tree vlan *vlan-list* [**detail**]

Use the command to check the spanning-tree status of the specified VLAN

Parameter

Parameter	Description
vlan-list	VLAN number list, such as: 1,2,3-10,15
detail	Displays the detailed information

Default

None

Usage guidelines

None

Command Mode

EXEC, global configuration mode or interface configuration mode

Example

The following examples to check the spanning-tree of vlan 1-2:

Switch_config#show spanning-tree vlan 1-2

Spanning tree enabled protocol PVST

VLAN0001

Root ID Priority 32769

Address 00E0.0FCC.F775

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```
    Bridge ID    Priority        32769
                 Address         00E0.0FCC.F775
                 Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

Interface            Role Sts Cost          Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
G0/1                 Desg FWD 19            128.1   P2p


VLAN0002
    Root ID      Priority        32770
                 Address         00E0.0FCC.F775
                 This bridge is the root
                 Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

    Bridge ID    Priority        32770
                 Address         00E0.0FCC.F775
                 Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

Interface            Role Sts Cost          Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
G0/1                 Desg FWD 19            128.1   P2p


Switch_config#
```

70.2.10 show spanning-tree pvst instance-list

Syntax

show spanning-tree pvst instance-list

Use the command to check how the PVST instance corresponds to the VLAN

Parameter

None

Default

None

Usage guidelines

None

Command Mode

EXEC, global configuration mode or interface configuration mode

Example

None

Chapter 71 RSTP Configuration Commands

71.1 RSTP Configuration Commands

71.1.1 spanning-tree mode rstp

Syntax

spanning-tree mode rstp

no spanning-tree mode

To enable the RSTP function, run spanning-tree mode rstp. To disable the RSTP, run no spanning-tree mode

Parameter

None

Default

RSTP is enabled

Usage Guidelines

None

Example

The following command shows how to enable rstp on switch

Switch_config# spanning-tree mode rstp

Switch_config#

71.1.2 spanning-tree rstp forward-time

Syntax

spanning-tree rstp forward-time *time*

no spanning-tree rstp forward-time

To configure the forwarding delay of RSTP, run **spanning-tree rstp forward-time** ***time***. To resume the default forwarding delay of RSTP, run **no spanning-tree rstp forward-time**

Parameter

Parameter	Description
time	Time of the forwarding delay whose value ranges between 4 and 30 seconds

Default

15s

Usage Guidelines

None

Example

The following example shows how to set the forwarding delay of RSTP to 20 seconds

Switch_config# spanning-tree rstp forward-time 20

Switch_config#

71.1.3 spanning-tree rstp hello-time

Syntax

spanning-tree rstp hello-time *time*

no spanning-tree rstp hello-time

To configure the update interval of RSTP, run **spanning-tree rstp hello-time** ***time***. To resume the default update interval of RSTP, run **no spanning-tree rstp hello-time**

Parameter

Parameter	Description
time	Update interval. The value ranges: 1-10s

Default

2s

Usage Guidelines

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch

Example

The following example shows how to set the update interval of RSTP to 8 seconds

Switch_config# spanning-tree rstp hello-time 8

Switch_config#

71.1.4 spanning-tree rstp max-age

Syntax

spanning-tree rstp max-age *time*

no spanning-tree rstp max-age

To configure the maximum lifespan of the RSTP BPDU, run **spanning-tree rstp max-age time**. To resume the default interval time, run **no spanning-tree rstp max-age**

Parameter

Parameter	Description
time	Maximum interval of the lifespan. Value ranges: 6-40s

Default

20s

Usage Guidelines

None

Example

The following example shows how to set the maximum lifespan of RSTP to 24 seconds

Switch_config# spanning-tree rstp max-age 24

Switch_config#

71.1.5 spanning-tree rstp priority

Syntax

spanning-tree rstp priority *value*

no spanning-tree rstp priority

To configure the RSTP priority value, run **spanning-tree rstp priority *value***. To resume the default value of the RSTP priority value, run **no spanning-tree rstp priority**

Parameter

Parameter	Description
value	Priority level of the bridge. The value ranges: 0-61440, step 4096

Default

32768

Usage Guidelines

None

Example

The following example shows how to configure the priority level of the brigde of rstp to 4096

Switch_config# spanning-tree rstp priority 4096

Switch_config#

71.1.6 spanning-tree rstp cost

Syntax

To configure the path cost of a port, run **spanning-tree rstp cost value**. To resume the default value, run **no spanning-tree rstp cost**

spanning-tree rstp cost *value*

no spanning-tree rstp cost

Parameter

Parameter	Description
value	Value of the path cost. The value ranges: 1-200000000

Default

The path cost depends on the connection rate of the port

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

Usage Guidelines

None

Example

The following example shows how to set the path cost of port g0/1 to 24:

Switch_config_g0/1# spanning-tree rstp cost 24

Switch_config_g0/1#

71.1.7 spanning-tree rstp port-priority

Syntax

To configure the priority level of a port, run **spanning-tree rstp port-priority *value***. To resume the default value, run **no spanning-tree rstp port-priority**

spanning-tree rstp port-priority *value*

no spanning-tree rstp port-priority

Parameter

Parameter	Description
value	Priority level of a port. The value ranges: 0-240, step 16

Default

128

Usage Guidelines

None

Example

The following example shows how to set the path cost of port g0/1 to 16:

Switch_config_g0/1# spanning-tree rstp port-priority 16

Switch_config_g0/1#

71.1.8 spanning-tree rstp edge

Syntax

To configure the edge port, run **spanning-tree rstp edge**. To return to the default setting, run **no spanning-tree rstp edge**

spanning-tree rstp edge

no spanning-tree rstp edge

Parameter

None

Default

Automatic check

Usage Guidelines

None

Command Mode

Interface configuration

Example

None

71.1.9 spanning-tree rstp point-to-point

Syntax

To set the point-to-point connection of a port to force-truce, force-false or auto, run this command

spanning-tree rstp point-to-point [force-true | force-false | auto]

Parameter

Parameter	Description
force-true	To set the point-to-point connection of a port to force-truce
force-false	To set the point-to-point connection of a port to force-false
auto	Sets the point-to-point connection to be automatic check (default)

Default

Automatic check

Usage Guidelines

None

Command Mode

Interface Configuration

Example

None

71.1.10 spanning-tree rstp migration-check

Syntax

To restart checking protocol transfer of RSTP, run **spanning-tree rstp migration-check**

spanning-tree rstp migration-check

Parameter

None

Default

None

Usage Guidelines

This command is used to restart the protocol transfer check on a port and to change the port in STP-compatible mode to the RSTP mode, enabling RSTP BPDU to be transmitted

Command Mode

Global and interface configuration

Example

The following example shows how to run protocol transfer check on interface G0/1:

Switch_config_g0/1#spanning-tree rstp migration-check

Switch_config_g0/1#

Chapter 72 MSTP Configuration Commands

72.1 MSTP Configuration Command

72.1.1 spanning-tree mode mstp

Syntax

To set the running mode of STP to **MSTP**, run **spanning-tree mode mstp**. To disable STP, Run **no spanning-tree mode**

spanning-tree mode mstp

no spanning-tree mode

Parameter

None

Default

The MSTP mode is disabled, while the RSTP mode is running

Usage Guidelines

None

Example

The following example shows how to enable MSTP protocol on the switch:

switch(config)# spanning-tree mode mstp

switch(config)#

72.1.2 spanning-tree mstp name

Syntax

spanning-tree mstp name *string*

no spanning-tree mstp name

To configure the regional name of the STP, run **spanning-tree mstp name *string***. To resume the default name, run **no spanning-tree mstp**

Parameter

Parameter	Description
String	Configures the character string of the name. The character string can have up to 32 characters, capital sensitive. The default value is in the form of character string like the MAC address of the switch

Default

Character string form of the switch's MAC address

Usage Guidelines

None

Example

The following example shows how to set the configuration name of the switch's STP to **reg-01**

switch(config)# spanning-tree mstp name reg-01

switch(config)#

72.1.3 spanning-tree mstp revision

Syntax

To generate the revision number of STP, run **spanning-tree mstp revision *value***. To return to the default value, run **no spanning-tree mstp revision**

spanning-tree mstp revision *value*

no spanning-tree mstp revision

Parameter

Parameter	Description
Value	Revision number: 0 ~65535. Its default value is 0

Default

The default value of the revision number is **0**

Usage Guidelines

None

Example

The following commands are used to set the regional revision number of STP to **100**

switch(config)# spanning-tree mstp revision 100

switch(config)#

72.1.4 spanning-tree mstp instance

Syntax

To map the VLAN to the MSTI, run **spanning-tree mstp instance** ***instance-id*** **vlan** ***vlan-list***. To re-map the VLAN to the CIST, run **no spanning-tree mstp instance** *instance-id*

spanning-tree mstp instance *instance-id* **vlan** *vlan-list*

no spanning-tree mstp instance *instance-id*

Parameter

Parameter	Description
instance-id	Instance number of the STP, meaning an MSTI which ranges from 1 to 15
vlan-list	VLAN list which is mapped to the STP, ranging from 1 to 4094

Default

All VLANs are mapped to the CIST (MST00)

Usage Guidelines

instance-id is an unique value representing an STP instance

vlan-list represents a VLAN group, such as "1,2,3", "1-5" and "1,2,5-10"

Example

The following commands map VLAN1 to instance 1 of STP, and VLAN5,7,10-20 to instance 2 of STP, and then re-map these VLANs to MST00

Switch_config# spanning-tree mstp instance 1 vlan 2

Switch_config# spanning-tree mstp instance 2 vlan 5,7,10-20

Switch_config# no spanning-tree mstp instance 1

Switch_config# no spanning-tree mstp instance 2

72.1.5 spanning-tree mstp root

Syntax

spanning-tree mstp *instance-id* **root** {**primary** | **secondary**}

[**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mstp *instance-id* **root**

To configure the specified MSTP instance to the primary/secondary root, run **spanning-tree mstp** *instance-id* **root** {**primary** | **secondary**}. To return to the default setting, run the negative form of the above command

Both the **diameter** command and the **hello-time** command can modify the network diameter and the **HelloTime** parameter of the MSTP when they are setting the root

Parameter

Parameter	Description
instance-id	MSTP instance, ranging from 0 to 15
primary	Sets the MSTP instance to the primary root
secondary	Sets the MSTP instance to the secondary root
net-diameter	Network diameter, which is optional When the instance-id parameter is 0, it is effective. It ranges from 2 to 7
seconds	Hello time, an optional parameter, which ranges from 1 to 10 seconds

Default

The priority value of all default roots of all MSTP instances are 32768, the network diameter is 7 and the HelloTime is 2 seconds

Usage Guidelines

Both the **diameter** command and the **hello-time** command are valid only when **instanc-id** is **0**

Generally, after you run the command to set the primary root, the protocol automatically checks the ID of the current network root and then sets the priority field of the root identifier to 24576 if this value gurantees the current OLT to be the root of the MSTP instance. If the priority value of the root is smaller than 24576, the protocol will automatically set the MSTP priority of the current root to a value which is 4096 smaller than the root's priority. Here, 4069 is the step of the root priority

Different from the configuration of the primary root, the protocol directly sets the MSTP priority of the OLT to **28672** after the command for configuring the secondary root is run. Thus, the current OLT can be the secondary root when the priorities of other OLTs are the default value **32768**

Example

The following commands are used to set the OLT to the primary root in the CIST and recalculate the time parameter of the MSTP through network diameter 3 and HelloTime3, and at last set the OLT to the secondary root in the MST01

Switch_config# spanning-tree mstp 0 root primary diameter 3 hello-time 3

Switch_config# spanning-tree mstp 1 root secondary

72.1.6 spanning-tree mstp priority

Syntax

To configure the bridge priority of the MSTP instance, run **spanning-tree mstp** *instance-id* **priority** *value*. To return to the default setting, run **no spanning-tree mstp** *instance-id* **priority**

spanning-tree mstp *instance-id* **priority** *value*

no spanning-tree mstp *instance-id* **priority**

Parameter

Parameter	Description
instance-id	MSTP instance number, ranging from 0 to 15
value	Bridge priority, which can be one of the given values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Default

The default priority of the bridges of all MSTP instances is 32768

Usage Guidelines

Each priority value in the MSTP instance is independent and can be configured independently

Example

The following commands are used to set the priority of the switch in the CIST and MST01 to 4096 and 8192 respectively

Switch_config# spanning-tree mstp 0 priority 4096

Switch_config# spanning-tree mstp 1 priority 8192

72.1.7 spanning-tree mstp hello-time

Syntax

spanning-tree mstp hello-time *seconds*

no spanning-tree mstp hello-time

It is used to configure the hello-time of the MSTP, and its negative form is used to resume the default settings of the HelloTime

Parameter

Parameter	Description
seconds	It ranges from 1 to 10 seconds. Its default value is 2 seconds

Default

2 seconds

Usage Guidelines

None

Example

The following commands are used to set the HelloTime of the MSTP to **10**

switch(config)# spanning-tree mstp hello-time 10

switch(config)# no spanning-tree mstp hello-time

72.1.8 spanning-tree mstp forward-time

Syntax

spanning-tree mstp forward-time *seconds*

no spanning-tree mstp forward-time

It is used to configure the Forward Delay of the MTSP. Its negative is used to resume the default settings

Parameter

Parameter	Description
seconds	It ranges from 4 to 30 seconds. Its default value is 15 seconds

Default

15 seconds

Usage Guidelines

None

Example

The following commands are used to set the **Forward Delay** parameter of the MTSP to **10**

Switch_config# spanning-tree mstp forward-time 10

Switch_config# no spanning-tree mstp forward-time

72.1.9 spanning-tree mstp max-age

Syntax

To configure the Max Age parameter of the MSTP, run **spanning-tree mstp max-age *seconds***. To return to the default setting, run the negative form of the command

spanning-tree mstp max-age *seconds*

no spanning-tree mstp max-age

Parameter

Parameter	Description
Seconds	Range: 6-40 seconds The default value is 20 seconds

Default

20 seconds

Usage Guidelines

None

Example

The following commands are used to set the **MaxAge** parameter of the MSTP to **10**

Switch_config# spanning-tree mstp max-age 10

Switch_config# no spanning-tree mstp max-age

72.1.10 spanning-tree mstp diameter

Syntax

To configure the network diameter of the MSTP, run **spanning-tree mstp diameter** ***net-diameter***. To return to the default setting, run **no spanning-tree mstp diameter**

spanning-tree mstp diameter *net-diameter*

no spanning-tree mstp diameter

Parameter	Description
net-diameter	Range: 2 - 7 Its default value is 7

Default

The default network diameter is 7

Usage Guidelines

The **net-diameter** parameter is not saved as an independent settings in the OLT. The time parameter that is modified through network diameter configuration can be saved. The **net-diameter** parameter is valid in the CIST. After settings, the three time parameters of the STP can be automatically updated to a relatively advantageous value

It is recommended to set the time parameters of the STP through root configuration or network diameter configuration. In this way, the reasonability of the time parameters can be assured

Example

The following first command is to set the bridge diameter of MSTP to 5. The second command is to resume the default value of the bridge diameter

Switch_config# spanning-tree mstp diameter 5

Switch_config# no spanning-tree mstp diameter

72.1.11 spanning-tree mstp max-hops

Syntax

spanning-tree mstp max-hops *hop-count*

no spanning-tree mstp max-hops

The **spanning-tree mstp max-hops** ***hop-count*** command is used to set the maximum number of hops of the MSTP BPDU

Its negative is used to resume the default settings

Parameter

Parameter	Description
hop-count	Ranges from: 6 -40 Its default value is 20

Default

The default vaue of the maximum hop counts is 20

Usage Guidelines

None

Example

The first command is to set the maximum hop counts of the MSTP BPDU to 6. The second command is to restore the default value of the maximum hop counts

Switch_config# spanning-tree mstp max-hops 6

Switch_config# no spanning-tree mstp max-hops

72.1.12 spanning-tree mstp port-priority

Syntax

To designate the priority of the spanning-tree STP instance, run **spanning-tree mstp** ***instance-id*** **port-priority**

value. To return to the default setting, run the no form of the command

spanning-tree mstp *instance-id* **port-priority** *value*

no spanning-tree *instance-id* **port-priority**

Parameter

Parameter	Description
instance-id	Number of the STP instance, ranging from 0 to 31
Value	Port priority, which is one of the following values: 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240

Default

The default priority value of the port in all STP instances is 128

Usage Guidelines

None

Example

The first command is to set the priority of port G0/1 in the CIST to 16. The second command is to resume the default value

Switch_config_g0/1# spanning-tree mstp 0 port-priority 16

Switch_config_g0/1# no spanning-tree mstp 0 port-priority

72.1.13 spanning-tree mstp cost

Syntax

The command **spanning-tree mstp *instance-id* cost value** is used to set the path cost of the port in the specified STP instance. Its negative is used to resume the default settings

spanning-tree mstp *instance-id* **cost** value

no spanning-tree mstp *instance-id* **cost**

Parameter

Parameter	Description
instance-id	Number of the STP instance, ranging from 0 to 15

value	Path cost of the port, ranging from 1 to 200000000

Default

It depends on the connection rate of the port:

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

Usage Guidelines

None

Example

The following commands are used to set the path cost of port G0/1 in the CIST to 200

Switch_config_g0/1# spanning-tree mstp 0 cost 200

Switch_config_g5/1#

72.1.14 spanning-tree mstp edge

Syntax

spanning-tree mstp edge

no spanning-tree mstp edge

To configure the edge port, run **spanning-tree mstp edge**. To return to the default setting, run **no spanning-tree mstp edge**.

Parameter

None

Default

Automatic check edge port

Usage Guidelines

None

Example

None

72.1.15 spanning-tree mstp point-to-point

Syntax

spanning-tree mstp point-to-point { **force-true** | **force-false** | **auto** }

no spanning-tree mstp point-to-point

To configure the connection type of a port, run **spanning-tree mstp point-to-point { force-true | force-false | auto }**. To resume the connection type to auto-check, run **no spanning-tree mstp point-to-point**

Parameter

Parameter	Description
force-true	Sets the port connection mode to point-to-point
force-false	Sets the port connection mode to sharing
auto	Sets the port connection mode to auto-chech (the default mode)

Default

MSTP will automatically check the port connection mode by default

Usage Guidelines

None

Example

The following example shows how to set the connection mode of port G0/1 to sharing.

Switch_config_g0/1# spanning-tree mstp point-to-point force-false

Switch_config_g0/1#

72.1.16 spanning-tree mstp mst-compatible

Syntax

spanning-tree mstp mst-compatible

no spanning-tree mstp mst-compatible

Enable/disable the MST-compatible mode, the global configuration mode

spanning-tree mstp mst-compatible {enable | disable}

no spanning-tree mstp mst-compatible

Enable/disable the MST-compatible mode, the interface configuration mode

Parameter

Parameter	Description

enable	Enable the MST-compatible mode
disable	Disable the MST-compatible mode

Default

The compitable mode is not activated by default and OLT cannot establish an area with other switches which transmit BPDU in compatible mode

Usage Guidelines

After the MST-compatible mode is enabled, configure other connected switches that are running other MSTP protocols to the roots of CIST, ensuring that the OLT can enter the MSTP-compatible mode by receiving the message

Example

The following command is to activate the MST-compatible mode in global configuration mode:

switch(config)#spanning-tree mstp mst-compatible

72.1.17 spanning-tree mstp migration-check

Syntax

spanning-tree mstp migration-check

Clear the STP information that is checked by the port, and restart the protocol conversion process

Parameter

None

Default

None

Usage Guidelines

The command is valid in global configuration mode and in port configuration mode

Example

The following commands are used to check the protocol conversion on all ports first, and then check the protocol conversion on port G0/1 again

Switch_config# spanning-tree mstp migration-check

Switch_config# interface g0/1

Switch_config_g0/1# spanning-tree mstp migration-check

72.1.18 spanning-tree mstp restricted-role

Syntax

[no] spanning-tree mstp restricted-role

Enable/disable the role restriction on the port

Parameter

None

Default

Disable the port's role restriction

Command Mode

Interface Configuration

Usage Guidelines

Enable the role restriction and the port will not be chosen as the root port

Example

None

72.1.19 spanning-tree mstp restricted-tcn

Syntax

[no] spanning-tree mstp restricted-tcn

Enable/disable the TCN restriction on the port

Parameter

None

Default

Disable the TCN restriction on the port

Command Mode

Interface Configuration

Usage Guidelines

Enable the TCN restriction on the port and do not tranmit topology changes to other ports

Example

None

72.1.20 show spanning-tree mstp

Syntax

show spanning-tree mstp [**instance** *instance-id*]

The command above is used to check the MSTP information. If you run the command **show spanning-tree mstp**, the information about all STP instances is displayed

Parameter

Parameter	Description
instance-id	Number of the STP instance, ranging from 0 to 15

Default

None

Usage Guidelines

It is valid in monitoring mode, global configuration mode or port mode

Example

The following shows how to view all STP instances through the command. Here, **MST00** stands for CIST, and the **Type** field stands for the port connection type

Switch#show spanning-tree mstp

MST00 Vlans Mapped: 1,4-4094

Bridge Address 00E0.0F64.8365 Priority 32768 (32768 mst-id 0)

Root This bridge is the CIST and regional root

Configured Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20

Root Times Hello Time 2, Forward Delay 15, Max Age 20

Interface Role Sts Cost Pri.Nbr Type

---------- ---- --- --------- ------- --------------------------------

G0/1 Desg FWD 200000 128.1 P2p

G0/2 Desg FWD 200000 128.2 Edge

MST01 Vlans Mapped: 2

Bridge Address 00E0.0F64.8365 Priority 32769 (32768 mst-id 1)

Root This bridge for MST01

Interface Role Sts Cost Pri.Nbr Type

---------- ---- --- --------- ------- --------------------------------

G0/1 Desg FWD 200000 128.1 P2p

MST02 Vlans Mapped: 3

Bridge Address 00E0.0F64.8365 Priority 32770 (32768 mst-id 2)

Root This bridge for MST02

Interface Role Sts Cost Pri.Nbr Type

---------- ---- --- --------- ------- --------------------------------

G0/1 Desg FWD 200000 128.1 P2p

72.1.21 show spanning-tree mstp region

Syntax

show spanning-tree mstp region

Check the regional configuration information about the MSTP

Parameter

None

Default

None

Usage Guidelines

None

Example

See the following information. **MST Config Table** shows the relation between VLAN and STP instance

switch(config)# show spanning-tree mstp region

MST Region:

Name: [reg01]

Revision:[0]

MST Config Table:

Instance VLAN IDs

---------- ----------

0 1,4-4094

1 2

2 3

72.1.22 show spanning-tree mstp detail

Syntax

show spanning-tree mstp detail

The command above is used to check the detailed information about MSTP

Parameter

None

Default

None

Usage Guidelines

None

Example

The following example shows the detailed STP information after the command is run, including the port connection type and optional characteristics:

Switch#show spanning-tree mstp detail

MST00 Vlans Mapped: 1,4-4094

Root Address 00E0.0F64.8365 Priority 32768 (32768 mst-id 0)

Root This root is the CIST and regional root

Configured Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20

Root Times Hello Time 2, Forward Delay 15, Max Age 20

FastEthernet0/1 of MST00 is designated forwarding

Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0

CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0

Designated Root Address 00E0.0F64.8365 Priority 32768 Port ID 128.1

Edge Port: disabled Link Type: point-to-point (auto)

Bpdu Guard: disabled (default) Root Guard: disabled (default)

Loop Guard: disabled (default)

Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec

Number of transitions to forwarding state: 1

Bpdu sent 335, received 5

FastEthernet0/3 of MST00 is backup blocking

Port Info Port ID 128.3 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0

CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0

Designated Root Address 00E0.0F64.8365 Priority 32768 Port ID 128.1

Edge Port: disabled Link Type: point-to-point (auto)

Bpdu Guard: disabled (default) Root Guard: disabled (default)

Loop Guard: disabled (default)

Timers: message expires in 5 sec, forward delay 15 sec, up time 662 sec

Number of transitions to forwarding state: 0

Bpdu sent 5, received 335

FastEthernet0/47 of MST00 is designated forwarding

Port Info Port ID 128.47 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0

CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0

Designated Root Address 00E0.0F64.8365 Priority 32768 Port ID 128.47

Edge Port: enabled (auto) Link Type: point-to-point (auto)

Bpdu Guard: disabled (default) Root Guard: disabled (default)

Loop Guard: disabled (default)

Timers: message expires in 0 sec, forward delay 0 sec, up time 1485 sec

Number of transitions to forwarding state: 1

Bpdu sent 744, received 0

MST01 Vlans Mapped: 2

Root Address 00E0.0F64.8365 Priority 32769 (32768 mst-id 1)

Root This root for MST01

FastEthernet0/1 of MST01 is designated forwarding

Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32769 Cost 0

Desingated Root Address 00E0.0F64.8365 Priority 32769 Port ID 128.1

Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec

Number of transitions to forwarding state: 1

MST Config Message transmitted 335, received 0

MST02 Vlans Mapped: 3

Root Address 00E0.0F64.8365 Priority 32770 (32768 mst-id 2)

Root This root for MST02

FastEthernet0/1 of MST02 is designated forwarding

Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32770 Cost 0

Desingated Root Address 00E0.0F64.8365 Priority 32770 Port ID 128.1

Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec

Number of transitions to forwarding state: 1

MST Config Message transmitted 335, received 0

72.1.23 show spanning-tree mstp interface

Syntax

show spanning-tree mstp interface *interface-id*

The command above is used to check the information about the port which is run under MSTP

Parameter

Parameter	Description
interface-id	Port name, such as "G0/1", "GigaEthernet0/2"

Default

None

Usage Guidelines

None

Example

The following example shows the information about port G0/1 after you run the command Switch#show spanning-tree mstp interface g0/1

GigaEthernet0/1 of MST00 is designated forwarding

Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0

CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0

Designated Bridge Address 00E0.0F64.8365 Priority 32768 Port ID 128.1

Edge Port: disabled Link Type: point-to-point (auto)

Bpdu Guard: disabled (default) Root Guard: disabled (default)

Loop Guard: disabled (default)

Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1

Bpdu sent 430, received 5

GigaEthernet0/1 of MST01 is designated forwarding

Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32769 Cost 0

Desingated Bridge Address 00E0.0F64.8365 Priority 32769 Port ID 128.1

Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1

MST Config Message transmitted 430, received 0

GigaEthernet0/1 of MST02 is designated forwarding

Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32770 Cost 0

Desingated Bridge Address 00E0.0F64.8365 Priority 32770 Port ID 128.1

Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1

MST Config Message transmitted 430, received 0

Instance Role Sts Cost Pri.Nbr Vlans Mapped

-------- ---- --- --------- ------- --------------------

0 Desg FWD 200000 128.1 1,4-4094

1 Desg FWD 200000 128.1 2

2 Desg FWD 200000 128.1 3

72.1.24 show spanning-tree mstp protocol-migration

Syntax

The command above is used to check the protocol conversion information when the port is running under MSTP

show spanning-tree mstp protocol-migration

Parameter

None

Default

None

Usage Guidelines

None

Example

The following example shows the information about protocol conversion after the command **show spanning-tree mstp protocol-migration** is run. Note that port G0/1 has transferred to the 802.1D STP mode

Switch#show spanning-tree mstp protocol-migration

MSTP Port Protocol Migration

```
Interface            Protocol
---------------- ---------- ------------
G0/1                  802.1D
```

Chapter 73 STP Optional Characteristic Configuration Commands

73.1 STP Optional Characteristic Configuration Commands

73.1.1 spanning-tree portfast

Syntax

To enable Port Fast features, use the **spanning-tree portfast** command in global configuration mode. To return to the default settings, use the no form of this command

spanning-tree portfast {bpdufilter | bpduguard | default}

no spanning-tree portfast {bpdufilter | bpduguard | default}

To enable Port Fast features, use the s **spanning-tree portfast** command in interface configuration mode. To return to the default settings, use the no form of this command

spanning-tree portfast [disable]

no spanning-tree portfast

Parameter

Parameter	Description
bpdufilter	Enables bpdu flter
bpduguard	Enables bpdu guard
default	Specifies the default method.

Default

Disabled

Usage Guidelines

In SSTP/PVST mode, the Port Fast characteristic makes a port immediately enter Forwarding state without experiencing any status change process. This configuration is invalid in RSTP/MSTP mode

After configuring Port Fast, BPDU Guard or BPDU Filter needs to be configured for protection

Command Mode

Global and interface configuration mode

Example

This example shows how to enable PortFast mode globally:

Switch(config)# spanning-tree portfast default

Switch(config)#

This example shows how to enable PortFast mode on the interface g0/1:

Switch_config_g0/1# spanning-tree portfast

Switch_config_g0/1#

73.1.2 spanning-tree bpduguard

Syntax

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration mode. To return to the default settings, use the no form of this command

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

Parameter

None

Default

Disabled

Usage Guidelines

In SSTP/PVST mode, if a port that configured BPDU Guard and Port Fast receives BPDU, this port will be forced to shutdown. User can restore it by the manual configuration. In RSTP/MSTP mode, if a port that configured BPDU Guard receives BPDU, this port will be configured to Blocking state for a period of time

Command Mode

Interface configuration

Example

This example shows how to enable BPDU guard on the interface G0/1:

Switch_config_g0/1# spanning-tree bpduguard enable

Switch_config_g0/1#

73.1.3 spanning-tree bpdufilter

Syntax

To enable bridge protocol data unit (BPDU) filtering on the interface, use the **spanning-tree bpdufilter** command in interface configuration mode. To return to the default settings, use the **no** form of this command

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

Parameter

None

Default

Disabled

Usage Guidelines

In SSTP/PVST mode, if a port that configured BPDU Filter and Port Fast receives BPDU, the BPDU Filter and Port Fast characteristics on that port will be disabled automatically to restore the port to an ordinary port. Then this port must endure the wait from Listening to Learning before entering Forwarding state

This feature is invalid in RSTP/MSTP mode

Command Mode

Interface configuration

Example

This example shows how to enable BPDU filtering on the interface G0/1:

Switch_config_g0/1# spanning-tree bpdufilter enable

Switch_config_g0/1#

73.1.4 spanning-tree uplinkfast

Syntax

To enable the debugging of the spanning-tree UplinkFast events, use the **spanning-tree uplinkfast** command. To disable the debugging output, use the no form of this command

spanning-tree uplinkfast

no spanning-tree uplinkfast

Parameter

None

Default

Disabled

Usage Guidelines

Uplink Fast characteristic is only valid in SSTP/PVST mode

Command Mode

Global configuration mode

Example

The following example enables uplinkfast characteristic:

Switch(config)# spanning-tree uplinkfast

Switch(config)#

73.1.5 spanning-tree backbonefast

Syntax

To enable debugging of the spanning-tree BackboneFast events, use the **spanning-tree backbonefast** command. To disable the debugging output, use the no form of this command

spanning-tree backbonefast

no spanning-tree backbonefast

Parameter

None

Default

Disabled

Usage Guidelines

Backbone Fast characteristic is only valid in SSTP/PVST mode

Command Mode

Global configuration mode

Example

The following command enables backbonefast characteristic:

Switch(config)# spanning-tree backbonefast

Switch(config)#

73.1.6 spanning-tree guard

Syntax

To enable or disable the guard mode, use the spanning-tree guard command in interface configuration mode. To return to the default settings, use the no form of this command

spanning-tree guard {loop | none | root}

no spanning-tree guard

Parameter

Parameter	Description
loop	Guard loop
none	Guard none
root	Guard root

Default

Disabled

Usage Guidelines

Root Guard characteristic can prevent a port from becoming Root port due to receving high priority BPDU

Loop Guard characteristic can protect a Root Port or a Alternate Port when it becomes the Designated Port. This function can prevent a port from occuring the loop when it cannot continuously receive BPDU

Command Mode

Interface configuration

Example

This example shows how to enable G0/1 to root guard:

Switch_config_g0/1# spanning-tree guard root

Switch_config_g0/1#

73.1.7 spanning-tree loopguard

Syntax

To enable loop guard as a default on all ports of a given bridge, use the **spanning-tree loopguard default** command in global configuration mode. To disable loop guard, use the **no** form of this command

spanning-tree loopguard default

Default

None

Usage Guidelines

None

Command Mode

Global configuration

Example

The following command enables loopguard function:

Switch(config)# spanning-tree loopguard default

Switch(config)#

73.1.8 spanning-tree loopfast

Syntax

spanning-tree loopfast

To configure Loop Fast, run **spanning-tree loopfast** in the global configuration mode. To return to the default setting, use the no form of this command

spanning-tree loopfast

spanning-tree loopfast disable

To configure Loop Fast, run **spanning-tree loopfast**. To return to the default setting, use the no form of this command

Parameter

None

Default

None

Usage Guidelines

Please configure this command under the guide of BDCOM's technical engineers

Command Mode

Global configuration and interface configuration

Example

The following example shows how to enable loopfast on the interface G0/1 in the global configuration mode and disable the function

Switch_config#spanning-tree loopfast

Switch_config#int g0/1

Switch_config_g0/1#spanning-tree loopfast disable

Switch_config_g0/1#exit

Switch_config#

73.1.9 spanning-tree fast-aging

Syntax

spanning-tree fast-aging

no spanning-tree fast-aging

The commands are used to enable/disable address table fast aging

spanning-tree fast-aging protection

no spanning-tree fast-aging protection

The commands are used to enable/disable address table fast aging protection

spanning-tree fast-aging protection time *value*

no spanning-tree fast-aging protection time

The commands are used to configure address table aging protection time

Parameter

Parameter	ParameterDescription
value	Aging protection time. The default is 15 seconds. The range is 10 to 60 seconds.

Default

Enable **fast-aging** and disable **protection** by default

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to enable fast aging protection and configure the protection time to 30s

Switch_config#spanning-tree fast-aging protection

Switch_config#spanning-tree fast-aging protection time 30

73.1.10 spanning-tree fast-aging flush-fdb

Syntax

spanning-tree fast-aging flush-fdb

no spanning-tree fast-aging flush-fdb

Enable/disable FDB-Flush

Parameter

None

Default

Enable FDB-Flush by default

Usage Guidelines

Please configure this command under the guide of BDCOM's technical engineers

FDB-Flush is independent of fast aging. FDB-Flush can be configured while **no spanning-tree fast-aging** is configured. Fast aging protection is invalid to FDB-Flush

Command Mode

Global configuration

Example

The following example shows how to disable fast-aging and enable FDB-Flush:

Switch_config#no spanning-tree fast-aging

Switch_config#spanning-tree fast-aging flush-fdb

73.1.11 spanning-tree bpdu-terminal

Syntax

spanning-tree bpdu-terminal

no spanning-tree bpdu-terminal

Enable/disable BPDU Terminal

Parameter

None

Default

Disable BPDU Terminal by default

Usage Guidelines

BPDU Terminal function can disable the forwarding of BPDU when no spanning tree is running

Command Mode

Global configuration mode

Example

The following example shows how to enable BPDU Terminal:

Switch_config#spanning-tree bpdu-terminal

Chapter 74 ime Range Configuration Commands

74.1 absolute

Syntax

[no] absolute { start *hour:minute day month year* **end** *hour:minute day month year*

| **start** *hour:minute day month year*

/**end** *hour:minute day month year***}**

To add or modify the absolute time in Time Range sub-mode, run the above commands. To return to the default setting, use the no form of this command

Parameters

Parameters	Description
hour	Hour in 24 hour system
minute	minute
day	day
month	month
year	year

Default Value

There is no default absolute time

Command Mode

Time Range sub-mode

Usage Guidelines

The absolute time takes effect from the current time if the start time is not configured;

The absolute time is valid forever if the end time is not configured

One time range can only have one absolute time. If the absolute time is already existed, the command can be used to modify it

Example

The following example shows how to configure the absolute time in the time range sub-mode

Switch_config_time_range_x#absolute start 8:08 8 8 2008 end 11:08 3 3 2010

Related Command

time-range

periodic

74.2 periodic

Syntax

[no] periodic { daily *hour:minute* **to** *hour:minute*

| weekdays *hour:minute* **to** *hour:minute*

| weekend *hour:minute* **to** *hour:minute*

| {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday} *hour:minute* **to** *hour:minute*

| {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday} *hour:minute* **to {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday}** *hour:minute* **}**

To add or modify the absolute time in Time Range sub-mode, run the above commands. To return to the default setting, use the no form of this command

Parameters

Parameters	Description
hour	Hour in 24 hour system
minute	minute

Default Value

There is no default absolute time

Command Mode

Time Range sub-mode

Usage Guidelines

The command can be used to configure the same item

Example

The following example shows how to add a period from 09:00 on Monday to 18:00 on Friday

Switch_config_time_range_x#periodic monday 09:00 to friday 18:00

The following example shows how to add a period from 12:00 to 13:00 every Tuesday, Thursday and Sunday.

Switch_config_time_range_x#periodic tuesday wednesday sunday 12:00 to 13:00

The following example shows how to add a period from 18:00 to 21:00 every workday

Switch_config_time_range_x#periodic weekdays 18:00 to 21:00

Related Command

time-range

absolute

74.3 show time-range

Syntax

show time-range [*name*]

To show the configuration of Time Range, run the above command. All configurations of Time Range will be shown in the system if the name is not specified. Otherwise, only TimeRange of specified name will be shown

Parameters

Parameters	Description
name	The character string of the Time Range name. The value ranges from 1 to 20 characters

Default Value

All Time Range configurations will be shown by default

Command Mode

EXEC, Global Configuration Mode, Time Range Sub-mode

Usage Guidelines

The result analysis of the command:

Take the result of the typical configuration as an example:

```
Switch_config#show time-range

Now: Date: 2008.3.4        Time: 13:16        Week: Tuesday

time-range entry: x (inactive)
        absolute start 12:00 1 January 2000 end 13:00 2 January 2008
```

```
            periodic weekdays    09:00 to 18:00

time-range entry: y (empty)

time-range entry: z (active)

            periodic daily          12:00 to 13:00

            periodic Monday         Thursday    Friday        08:00 to 09:00

            periodic Saturday    15:00 to Sunday        20:00

            periodic daily          09:00 to 18:00


Switch_config#
```

In the first line shows "Now: Date: 2008.3.4 Time: 13:16 Week: Tuesday", which means the date is 4th May, 2008; the time is 13:16; the day is Tuesday

Subsequently the screen shows the configuration and status of Time Ranges which named x, y and z respectively. Time Range x has two items: absolute time and period, and it is in the inactive state; Time Range y has no item and it is in the empty state; Time Range z has 4 periods and it is in active state

Example

The following example shows how to show the configuration of the time range named a

```
Switch_config#show time-range a


Now: Date: 2008.3.4          Time: 14:01          Week: Tuesday


time-range entry: a (inactive)

            periodic Monday        12:00 to 13:00


Switch_config#
```

74.4 time-range

Syntax

[no] time-range *name*

To add a Time Range named name in the global configuration mode. To return to the default setting, use the no form of this command

Parameters

Parameters	Description
name	The character string of the Time Range name. The value ranges from 1 to 20 characters

Default Value

Time Range is not used by default

Command Mode

Global configuration mode

Usage Guidelines

If the corresponding Time Range is not existed, a Time Range will be created in time range configuration mode.
If the corresponding Time Range is already existed, it will enter the time range configuration mode directly

Example

The following example shows how to configure a time range named a

Switch_config#time-range a

Switch_config_time_range_a#

74.5 debug time-range

Syntax

debug time-range

To enable the debug switch of Time Range, run the above commands

Parameters

None

Default Value

The debug switch of the Time Range is disabled by default

Command Mode

EXEC

Usage Guidelines

Time Range Debug Output Information Analysis

Take the typical debug output information as an example:

```
Switch_config_time_range_a#Mar    4 14:01:18 Timerange(x) gains waiting second = 42949672

Mar    4 14:01:18 Timerange(x) PRE_STATE: [INACTIVE], CUR_STATE: [INACTIVE], CHANGE: [unCHANGED]
```

```
Mar    4 14:01:18 Timerange(y) gains waiting second = 42949672

Mar    4 14:01:18 Timerange(y) PRE_STATE: [EMPTY], CUR_STATE: [EMPTY], CHANGE: [unCHANGED]

Mar    4 14:01:18 Timerange(z) gains waiting second = 14408

Mar    4 14:01:18 Timerange(z) PRE_STATE: [ACTIVE], CUR_STATE: [ACTIVE], CHANGE: [unCHANGED]

Mar    4 14:01:18 Timerange(X) gains waiting second = 424749

Mar    4 14:01:18 Timerange(X) PRE_STATE: [INACTIVE], CUR_STATE: [INACTIVE], CHANGE: [unCHANGED]

Mar    4 14:01:18 Timerange(a) gains waiting second = 511149

Mar    4 14:01:18 Timerange(a) PRE_STATE: [INACTIVE], CUR_STATE: [INACTIVE], CHANGE: [CHANGED]


Switch_config_time_range_a#Mar    4 14:01:18 WHOLE time-range will be checked after waiting ticks =
1440800
```

The above information shows the current information of all Time Ranges. Their name are x, y, z, X or a

The information "Mar 4 14:01:18 Timerange(x) gains waiting second = 42949672" means the time difference between 14:01:18, 4th March and next moment of checking the effectiveness of Time Range x is 42949672 seconds

The information "Mar 4 14:01:18 Timerange(x) PRE_STATE: [INACTIVE], CUR_STATE: [INACTIVE], CHANGE: [unCHANGED]"means at 14:01:18, 4th March, the pre-state (PRE_STATE) of Time Range x is INACTIVE; the current state (CUR_STATE) is INACTIVE and the status is (unCHANGED)

The information "Mar 4 14:01:18 WHOLE time-range will be checked after waiting ticks = 1440800" means the difference between 14:01:18, 4th March and next check of Time Range of the whole system is 1440800 ticks. (tick is a time unit in the PC system; 1 tick=10ms)

Chapter 75 UDLD Configuration Commands

75.1 udld enable

Syntax

udld enable

To enable global UDLD function in normal mode, use **udld enable** command

no udld enable

To disable global UDLD function in normal mode, use **no udld enable** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of all interfaces in normal mode. In normal mode, if cannot connect, UDLD will set the interface in the state of undetermined, without disabling the interface protocol. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Global configuration mode

Example

The following example shows how to enable UDLD in normal mode:

Switch_config#udld enable

75.2 udld aggressive

Syntax

udld aggressive

To enable global UDLD function in aggressive mode, use **udld aggressive** command

no udld aggressive

To disable global UDLD function in aggressive mode, use **udld aggressive** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of all interfaces in aggressive mode. In aggressive mode, if UDLD cannot connect and fail to reconnect, there is consider to be serious network problem for communication interruption. Then UDLD will disable the interface protocol and the interface is in the state of errdisable. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Global configuration mode

Example

The following example shows how to enable UDLD in aggressive mode:

Switch_config#udld aggressive

75.3 udld port

Syntax

udld port

To enable UDLD function of the port in normal mode, use **udld port** command

no udld port

To disable UDLD function of the port in normal mode, use **no udld port** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of its interface in normal mode. In normal mode, if cannot connect, UDLD will set the interface in the state of undetermined, without disabling the interface protocol. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Interface configuration mode

Example

The following example shows how to enable UDLD of the port in normal mode:

Switch_config_g0/1#udld port

75.4 udld port aggressive

Syntax

udld port aggressive

To enable UDLD function of the port in aggressive mode, use **udld port aggressive** command

no udld port aggressive

To disable UDLD function of the port in aggressive mode, use **no udld port aggressive** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of its interface in aggressive mode. In aggressive mode, if UDLD cannot connect and fail to reconnect, there is consider to be serious network problem for communication interruption. Then UDLD will disable the interface protocol and the interface is in the state of errdisable. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Interface configuration mode

Example

The following example shows how to enable UDLD of the port in aggressive mode:

Switch_config_g0/1#udld port aggressive

75.5 udld message

Syntax

udld message *time*

To set udld message intervals in aggressive mode, use above command

no udld message

To return to the default setting, use the no form of this command

Parameter

Parameter	Description
time	Interval time in aggressive mode, range: 7-90s

Default

15s

Usage Guidelines

Set the udld message interval in aggressive mode. Only after restarting the aggressive mode, new interval time can be valid

Command Mode

Global configuration mode

Example

The following example shows how to set the udld message interval in aggressive mode as 7s, which is valid after restarting the aggressive mode:

Switch_config#udld message 7

75.6 udld reset

Syntax

udld reset

To reset the interface disabled by UDLD mode protocol, use above command

Parameter

None

Default

None

Usage Guidelines

Reset the interface disabled by UDLD mode protocol

Command Mode

Management configuration mode

Example

The following example shows how to reset the interface disabled by UDLD module:

Switch#udld reset

1 ports shutdown by UDLD were reset

%%UDLD-2-UDLD_PORT_RESET: UDLD reset interface GigaEthernet0/1

%%PM-4-ERR_RECOVER: Attempting to recover from udld err-disable state on GigaEthernet0/1

75.7 show udld

Syntax

show udld interface [*interface*]

To display the connection information of running UDLD, use above command

Parameter

Parameter	Description
interface	Display UDLD operation information of the specified interface

Default

None

Usage Guidelines

Display the operation information of UDLD module. When not input the interface parameter, UDLD operation information of all interfaces will be displayed. When input the interface parameter, only display the UDLD information of the interface whose parameter is input

Command Mode

Management/Global configuration mode

Example

The following example shows how to display the operation state information of UDLD module in all interfaces:

Switch_config#show udld

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

Interface GigaEthernet0/2

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

Interface GigaEthernet0/3

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

....

....

....

The following example shows how to display the operation state information of UDLD module in thterface G0/1:

Switch_config#show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

```
Switch_config#
```

Chapter 76 Urpf Configuration Commands

76.1 urpf check(Global)

Syntax

Enable/disable uRPF check in the global mode, run the following command

[no] urpf check

Parameter

None

Default value

Disabled

Command mode

Global configuration mode

Usage guidelines

The command can be effective only uRPF mode is enabled under the port of Urpf in the global mode

Example

None

Related command

None

76.2 urpf check(VLAN interface)

Syntax

Set uPRF check mode under the mode of VLAN, run the following command

urpf check *mode [uncheck_default_route]*

no urpf check

Parameter

Parameter	Description
mode	Configures uRPF check mode, strict or loose
uncheck_default_route	After check uPRF, FIB entries will not be checked if they are default route

Default value

Disabled under the port of VLAN

Command mode

Interface configuration mode

Usage guidelines

Configuring uRPF check mode under the port of VLAN can be effective only when uRPF check is enabled in the global mode

Example

The following example shows how to configure uRPF strict check mode and enable the fitted FIB entries as the default route

urpf check strict uncheck_default_route

Related command

show interface

Show uRPF check statistics

Chapter 77 UDLD Configuration Commands

77.1 udld enable

Syntax

udld enable

To enable global UDLD function in normal mode, use **udld enable** command

no udld enable

To disable global UDLD function in normal mode, use **no udld enable** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of all interfaces in normal mode. In normal mode, if cannot connect, UDLD will set the interface in the state of undetermined, without disabling the interface protocol. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Global configuration mode

Example

The following example shows how to enable UDLD in normal mode:

Switch_config#udld enable

77.2 udld aggressive

Syntax

udld aggressive

To enable global UDLD function in aggressive mode, use **udld aggressive** command

no udld aggressive

To disable global UDLD function in aggressive mode, use **udld aggressive** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of all interfaces in aggressive mode. In aggressive mode, if UDLD cannot connect and fail to reconnect, there is consider to be serious network problem for communication interruption. Then UDLD will disable the interface protocol and the interface is in the state of errdisable. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Global configuration mode

Example

The following example shows how to enable UDLD in aggressive mode:

Switch_config#udld aggressive

77.3 udld port

Syntax

udld port

To enable UDLD function of the port in normal mode, use **udld port** command

no udld port

To disable UDLD function of the port in normal mode, use **no udld port** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of its interface in normal mode. In normal mode, if cannot connect, UDLD will set the interface in the state of undetermined, without disabling the interface protocol. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Interface configuration mode

Example

The following example shows how to enable UDLD of the port in normal mode:

Switch_config_g0/1#udld port

77.4 udld port aggressive

Syntax

udld port aggressive

To enable UDLD function of the port in aggressive mode, use **udld port aggressive** command

no udld port aggressive

To disable UDLD function of the port in aggressive mode, use **no udld port aggressive** command

Parameter

None

Default

None

Usage Guidelines

Enable UDLD function of its interface in aggressive mode. In aggressive mode, if UDLD cannot connect and fail to reconnect, there is consider to be serious network problem for communication interruption. Then UDLD will disable the interface protocol and the interface is in the state of errdisable. If the UDLD is thought to be a two-way link, then the interface is in state of Bidirectional

Command Mode

Interface configuration mode

Example

The following example shows how to enable UDLD of the port in aggressive mode:

Switch_config_g0/1#udld port aggressive

77.5 udld message

Syntax

udld message *time*

To set udld message intervals in aggressive mode, use above command

no udld message

To return to the default setting, use the no form of this command

Parameter

Parameter	Description
time	Interval time in aggressive mode, range: 7-90s

Default

15s

Usage Guidelines

Set the udld message interval in aggressive mode. Only after restarting the aggressive mode, new interval time can be valid

Command Mode

Global configuration mode

Example

The following example shows how to set the udld message interval in aggressive mode as 7s, which is valid after restarting the aggressive mode:

Switch_config#udld message 7

77.6 udld reset

Syntax

udld reset

To reset the interface disabled by UDLD mode protocol, use above command

Parameter

None

Default

None

Usage Guidelines

Reset the interface disabled by UDLD mode protocol

Command Mode

Management configuration mode

Example

The following example shows how to reset the interface disabled by UDLD module:

Switch#udld reset

1 ports shutdown by UDLD were reset

%%UDLD-2-UDLD_PORT_RESET: UDLD reset interface GigaEthernet0/1

%%PM-4-ERR_RECOVER: Attempting to recover from udld err-disable state on GigaEthernet0/1

77.7 show udld

Syntax

show udld interface [*interface*]

To display the connection information of running UDLD, use above command

Parameter

Parameter	Description
interface	Display UDLD operation information of the specified interface

Default

None

Usage Guidelines

Display the operation information of UDLD module. When not input the interface parameter, UDLD operation information of all interfaces will be displayed. When input the interface parameter, only display the UDLD information of the interface whose parameter is input

Command Mode

Management/Global configuration mode

Example

The following example shows how to display the operation state information of UDLD module in all interfaces:

Switch_config#show udld

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

Interface GigaEthernet0/2

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

Interface GigaEthernet0/3

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

....

....

....

The following example shows how to display the operation state information of UDLD module in thterface G0/1:

Switch_config#show udld interface g0/1

Interface GigaEthernet0/1

Port enable administrative configuration setting: Enabled

Port enable operational state: Enabled

Current bidirectional state: Unknown

Current operational state: Link down

Message interval: 15

Time out interval: 1

No neighbor cache information stored

Switch_config#