CLI Reference Guide

DeltaStream Chassis Optical Line Terminal

1900002969 REV1.0.0

May 2026

© 2026 TP-Link

CONTENTS

Preface 1

Chapter 1 Using the CLI 2

1.1 Accessing the CLI 2
1.1.1 Via the Console Port 2
1.1.2 Logon by Telnet 3
1.1.3 Logon by SSH 5
1.2 CLI Command Modes 10
1.3 Privilege Restrictions 12
1.4 Conventions 13
1.4.1 Format Conventions 13
1.4.2 Special Characters 13
1.4.3 Parameter Format 13

Chapter 2 User Interface 15

2.1 enable 15
2.2 service password-encryption 15
2.3 enable password 16
2.4 enable secret 17
2.5 configure 18
2.6 exit 19
2.7 end 19
2.8 clipaging 20
2.9 history 20
2.10 history clear 21

Chapter 3 User Management Commands 22

3.1 user name (password) 22
3.2 user name (secret) 23
3.3 show user account-list 25
3.4 show user configuration 25

Chapter 4 Management Port Configuration Commands 26

4.1 description 26
4.2 ip 26
4.3 ipv6 27
4.4 shutdown 28

4.5 clear 28
4.6 end 29
4.7 exit 30
4.8 history 30
4.9 no 31

Chapter 5 System Configuration Commands 32

5.1 system-time manual 32
5.2 system-time ntp 32
5.3 system-time dst predefined 34
5.4 system-time dst date 35
5.5 system-time dst recurring 36
5.6 hostname 37
5.7 location 38
5.8 contact-info 38
5.9 led 39
5.10 ip address 39
5.11 ip address-alloc 40
5.12 reset 41
5.13 service reset-disable 42
5.14 reboot 42
5.15 reboot-schedule 43
5.16 copy running-config startup-config 44
5.17 copy startup-config tftp 44
5.18 copy tftp startup-config 45
5.19 copy backup-config tftp 45
5.20 copy backup-config startup-config 46
5.21 copy running-config backup-config 47
5.22 copy tftp backup-config 47
5.23 boot application 48
5.24 boot config 48
5.25 firmware upgrade 49
5.26 ping 50
5.27 tracert 51
5.28 show system-info 52
5.29 show image-info 53
5.30 show boot 53
5.31 show running-config 54

5.32 show startup-config 54
5.33 show system-time 55
5.34 show system-time dst 55
5.35 show system-time ntp 56
5.36 show cpu-utilization 56
5.37 show memory-utilization 57
5.38 dpms remote-address 57
5.39 dpms interface-id 58
5.40 show dpms remote-address 59
5.41 show dpms interface 59
5.42 patch load 60
5.43 patch active 61
5.44 patch run 61
5.45 patch deactive 62
5.46 patch uninstall 63
5.47 patch delete 63
5.48 show patch information 64

Chapter 6 Time Range Commands 65

6.1 time-range 65
6.2 absolute 65
6.3 periodic 66
6.4 holiday (time-range mode) 67
6.5 holiday 68
6.6 show holiday 68
6.7 show time-range 69

Chapter 7 PON Port Configuration Commands 70

7.1 shutdown 70
7.2 downstream-fec 70
7.3 key-exchange 71
7.4 dba-calculate-mode 72
7.5 range 73
7.6 long-laseront auto-detect 73
7.7 long-laseront auto-detect-interval 74
7.8 long-laseront auto-isolate 75
7.9 onu-isolate 75
7.10 port-isolate 76

7.11 show interface gpon 76
Chapter 8 DBA Profile Configuration Commands 78
8.1 dba-profile 78
8.2 show dba-profile 80
Chapter 9 Line Profile Configuration Commands 81
9.1 ont-lineprofile gpon 81
9.2 tcont 82
9.3 mapping mode 82
9.4 gem add 83
9.5 gem mapping 84
9.6 fec-upstream 85
9.7 omcc encrypt 86
9.8 show ont-lineprofile gpon 87
9.9 show ont-lineprofile gpon bound-info 87
Chapter 10 Service Profile Configuration Commands 89
10.1 ont-srvprofile gpon 89
10.2 ont-port 90
10.3 mac-learning 91
10.4 native-vlan 91
10.5 multicast-mode 92
10.6 multicast-forward 93
10.7 priority-policy 94
10.8 port igmp-forward 95
10.9 port q-in-q 96
10.10 max-mac-count 96
10.11 port vlan 97
10.12 show ont-srvprofile gpon 98
10.13 show ont-srvprofile gpon bound-info 99
Chapter 11 Traffic Profile Configuration Commands 100
11.1 traffic-profile 100
11.2 show traffic-profile 100
Chapter 12 Management Profile Configuration Commands 102
12.1 ont-mgmtprofile 102
12.2 catv 103

12.3 sipuser 103
12.4 wlan 104
12.5 wan 106
12.6 cwmp 108
12.7 show ont-mgmtprofile gpon 110
12.8 show ont-mgmtprofile gpon bound-info 111
12.9 remote-access 111

Chapter 13 ONU-Register Commands 113

13.1 ont autofind 113
13.2 ont autofind timeout 113
13.3 ont autofind interval 114
13.4 ont cancel 114
13.5 ont confirm 115
13.6 ont confirm all 117
13.7 show ont autofind 119
13.8 ont add 120
13.9 ont activate 122
13.10 ont reset 123
13.11 ont delete 124
13.12 show ont auth-info 124
13.13 ont auto-auth 126
13.14 ont auto-auth match-mode 126
13.15 ont auto-auth authmode 127
13.16 ont auto-auth rule 128
13.17 show ont auto-auth 129
13.18 ont re-register 130
13.19 ont reboot 130

Chapter 14 ONU-Management Commands 132

14.1 ont port attribute admin-status 132
14.2 ont port native-vlan 132
14.3 ont port attribute speed 133
14.4 ont port attribute duplex 134
14.5 ont port attribute flow-control 134
14.6 ont port car 135
14.7 show ont port attribute 136
14.8 show ont port state 136

14.9 ont wan 137
14.10 ont wan admin-status 140
14.11 show ont wan 141
14.12 ont upgrade 142
14.13 ont upgrade ftp 142
14.14 ont upgrade filename 143
14.15 ont upgrade set 143
14.16 ont upgrade stop 144
14.17 show ont upgrade info 145
14.18 show ont upgrade progress 145
14.19 ont modify profile 146
14.20 ont modify authmode 147
14.21 ont modify description 148
14.22 show ont capability 149
14.23 show ont config-capability 149
14.24 show ont failed-config 150
14.25 show ont info 150
14.26 show ont optical-info 151
14.27 show ont version 152
14.28 show ont register-statistics 152
14.29 ont iphost 153
14.30 show ont iphost 154
14.31 ont sipuser 155
14.32 show ont sipuser 156
14.33 ont wlan 157
14.34 show ont wlan 158
14.35 ont catv 159
14.36 show ont catv 160
14.37 ont cwmp 161
14.38 ont cwmp-auth-profile 162
14.39 show ont cwmp 163
14.40 ont isolation 163
14.41 show ont isolation 164
14.42 show ont learned-mac 165
14.43 ont remote-access 166
14.44 show ont remote-access 166

Chapter 15 Service Port Configuration Commands 168

15.1 service-port 168
15.2 show service-port 170
15.3 auto-service-port 171
15.4 show auto-service-port 172

Chapter 16 Ethernet Port Configuration Commands 174

16.1 interface gigabitEthernet 174
16.2 interface range gigabitEthernet 174
16.3 description 175
16.4 shutdown 176
16.5 flow-control 177
16.6 fec-mode 177
16.7 duplex 178
16.8 jumbo-size 179
16.9 speed 179
16.10 clear counters 180
16.11 show fiber-ports 180
16.12 show interface status 181
16.13 show interface counters 181
16.14 show interface configuration 182

Chapter 17 Port Isolation Commands 184

17.1 port isolation 184
17.2 show port isolation interface 185

Chapter 18 Loopback Detection Commands 186

18.1 loopback-detection (global) 186
18.2 loopback-detection interval 186
18.3 loopback-detection recovery-time 187
18.4 loopback-detection (interface) 188
18.5 loopback-detection config process-mode 188
18.6 loopback-detection recover 189
18.7 show loopback-detection global 190
18.8 show loopback-detection interface 190

Chapter 19 DDM Commands 192

19.1 ddm state enable 192
19.2 ddm shutdown 192

19.3 ddm temperature_threshold 193
19.4 ddm voltage_threshold 194
19.5 ddm bias_current_threshold 195
19.6 ddm tx_power_threshold 196
19.7 ddm rx_power_threshold 197
19.8 show ddm configuration 198
19.9 show ddm status 199

Chapter 20 Etherchannel Commands 200

20.1 channel-group 200
20.2 port-channel load-balance 201
20.3 lacp system-priority 202
20.4 lacp port-priority 203
20.5 show etherchannel 203
20.6 show etherchannel load-balance 204
20.7 show lacp 205
20.8 show lacp sys-id 205

Chapter 21 MAC Address Commands 207

21.1 mac address-table static 207
21.2 no mac address-table dynamic 208
21.3 mac address-table aging-time 208
21.4 mac address-table filtering 209
21.5 mac address-table max-mac-count 210
21.6 show mac address-table 211
21.7 clear mac address-table 212
21.8 show mac address-table aging-time 212
21.9 show mac address-table max-mac-count 213
21.10 show mac address-table interface 213
21.11 show mac address-table count 214
21.12 show mac address-table address 214
21.13 show mac address-table vlan 215

Chapter 22 IEEE 802.1Q VLAN Commands 216

22.1 vlan 216
22.2 interface vlan 216
22.3 name 217
22.4 switchport general allowed vlan 218
22.5 switchport pvid 218

22.6 switchport check ingress 219
22.7 switchport acceptable frame 220
22.8 show vlan summary 220
22.9 show vlan brief 221
22.10 show vlan 221
22.11 show interface switchport 222

Chapter 23 MAC-based VLAN Commands 223

23.1 mac-vlan mac-address 223
23.2 mac-vlan 224
23.3 show mac-vlan 224
23.4 show mac-vlan interface 225

Chapter 24 Protocol-based VLAN Commands 226

24.1 protocol-vlan template 226
24.2 protocol-vlan vlan 227
24.3 protocol-vlan group 228
24.4 show protocol-vlan template 228
24.5 show protocol-vlan vlan 229

Chapter 25 GVRP Commands 230

25.1 gvrp 230
25.2 gvrp (interface) 230
25.3 gvrp registration 231
25.4 gvrp timer 232
25.5 show gvrp interface 233
25.6 show gvrp global 234

Chapter 26 IGMP Snooping Commands 235

26.1 ip igmp snooping (global) 235
26.2 ip igmp snooping version 235
26.3 ip igmp snooping drop-unknown 236
26.4 ip igmp snooping header-validation 237
26.5 ip igmp snooping vlan-config 237
26.6 ip igmp snooping vlan-config (immediate-leave) 239
26.7 ip igmp snooping vlan-config (report-suppression) 239
26.8 ip igmp snooping vlan-config (router-ports-forbidden) 240
26.9 ip igmp snooping vlan-config (rport interface) 241
26.10 ip igmp snooping vlan-config (static) 242

26.11 ip igmp snooping vlan-config (querier) 243
26.12 ip igmp snooping (interface) 244
26.13 ip igmp snooping max-groups 245
26.14 ip igmp snooping immediate-leave 246
26.15 ip igmp profile 246
26.16 deny 247
26.17 permit 247
26.18 range 248
26.19 ip igmp filter 249
26.20 clear ip igmp snooping statistics 249
26.21 show ip igmp snooping 250
26.22 show ip igmp snooping interface 250
26.23 show ip igmp snooping vlan 251
26.24 show ip igmp snooping groups 252
26.25 show ip igmp profile 253

Chapter 27 MLD Snooping Commands 254

27.1 ipv6 mld snooping (global) 254
27.2 ipv6 mld snooping drop-unknown 254
27.3 ipv6 mld snooping vlan-config 255
27.4 ipv6 mld snooping vlan-config (immediate-leave) 256
27.5 ipv6 mld snooping vlan-config (report-suppression) 257
27.6 ipv6 mld snooping vlan-config (router-ports-forbidden) 258
27.7 ipv6 mld snooping vlan-config (rport interface) 259
27.8 ipv6 mld snooping vlan-config (static) 259
27.9 ipv6 mld snooping vlan-config (querier) 260
27.10 ipv6 mld snooping (interface) 262
27.11 ipv6 mld snooping max-groups 262
27.12 ipv6 mld snooping immediate-leave 264
27.13 ipv6 mld profile 264
27.14 deny 265
27.15 permit 265
27.16 range 266
27.17 ipv6 mld filter 267
27.18 clear ipv6 mld snooping statistics 267
27.19 show ipv6 mld snooping 268
27.20 show ipv6 mld snooping interface 268
27.21 show ipv6 mld snooping vlan 269

27.22 show ipv6 mld snooping groups 270
27.23 show ipv6 mld profile 270

Chapter 28 MVR Commands 272

28.1 mvr (global) 272
28.2 mvr group 272
28.3 mvr mode 273
28.4 mvr querytime 274
28.5 mvr vlan 275
28.6 mvr (interface) 275
28.7 mvr type 276
28.8 mvr immediate 277
28.9 mvr vlan (group) 277
28.10 show mvr 278
28.11 show mvr interface 279
28.12 show mvr members 279

Chapter 29 MSTP Commands 281

29.1 debug spanning-tree 281
29.2 spanning-tree (global) 282
29.3 spanning-tree (interface) 282
29.4 spanning-tree common-config 283
29.5 spanning-tree mode 284
29.6 spanning-tree mst configuration 285
29.7 instance 285
29.8 name 286
29.9 revision 287
29.10 spanning-tree mst instance 288
29.11 spanning-tree mst 288
29.12 spanning-tree priority 289
29.13 spanning-tree timer 290
29.14 spanning-tree hold-count 291
29.15 spanning-tree max-hops 291
29.16 spanning-tree bpdufilter 292
29.17 spanning-tree bpduflood 293
29.18 spanning-tree bpduguard 293
29.19 spanning-tree guard loop 294
29.20 spanning-tree guard root 295

29.21 spanning-tree guard tc 295
29.22 spanning-tree mcheck 296
29.23 show spanning-tree active 296
29.24 show spanning-tree bridge 297
29.25 show spanning-tree interface 297
29.26 show spanning-tree interface-security 298
29.27 show spanning-tree mst 299

Chapter 30 LLDP Commands 301

30.1 lldp 301
30.2 lldp forward_message 301
30.3 lldp hold-multiplier 302
30.4 lldp timer 303
30.5 lldp receive 304
30.6 lldp transmit 304
30.7 lldp snmp-trap 305
30.8 lldp tlv-select 306
30.9 lldp management-address 306
30.10 lldp med-fast-count 307
30.11 lldp med-status 308
30.12 lldp med-tlv-select 308
30.13 lldp med-location 309
30.14 show lldp 310
30.15 show lldp interface 310
30.16 show lldp local-information interface 311
30.17 show lldp neighbor-information interface 312
30.18 show lldp traffic interface 312

Chapter 31 Static Routes Commands 314

31.1 ip routing 314
31.2 interface vlan 314
31.3 interface loopback 315
31.4 switchport 315
31.5 interface range port-channel 316
31.6 description 317
31.7 shutdown 317
31.8 interface port-channel 318
31.9 ip route 319

31.10 ipv6 routing 319
31.11 ipv6 route 320
31.12 show interface vlan 321
31.13 show ip interface 321
31.14 show ip interface brief 322
31.15 show ip route 322
31.16 show ip route specify 323
31.17 show ip route summary 324
31.18 show ipv6 interface 324
31.19 show ipv6 route 325
31.20 show ipv6 route summary 325

Chapter 32 IPv6 Address Configuration Commands 327

32.1 ipv6 enable 327
32.2 ipv6 address autoconfig 327
32.3 ipv6 address link-local 328
32.4 ipv6 address dhcp 329
32.5 ipv6 address ra 329
32.6 ipv6 address eui-64 330
32.7 ipv6 address 331
32.8 show ipv6 interface 332

Chapter 33 ARP Commands 333

33.1 arp 333
33.2 clear arp-cache 334
33.3 arp dynamicrenew 334
33.4 arp timeout 335
33.5 gratuitous-arp intf-status-up enable 335
33.6 gratuitous-arp dup-ip-detected enable 336
33.7 gratuitous-arp learning enable 336
33.8 gratuitous-arp send-interval 337
33.9 ip proxy-arp 338
33.10 ip local-proxy-arp 338
33.11 show arp 339
33.12 show ip arp (interface) 340
33.13 show ip arp summary 340
33.14 show gratuitous-arp 341
33.15 show ip proxy-arp 341

33.16 show ip local-proxy-arp 342

Chapter 34 DHCP Server Commands 343

34.1 service dhcp server 343
34.2 ip dhcp server extend-option capwap-ac-ip 343
34.3 ip dhcp server extend-option vendor-class-id 344
34.4 ip dhcp server exclude-address 345
34.5 ip dhcp server pool 345
34.6 ip dhcp server ping timeout 346
34.7 ip dhcp server ping packets 347
34.8 network 347
34.9 lease 348
34.10 address hardware-address 349
34.11 address client-identifier 350
34.12 default-gateway 350
34.13 dns-server 351
34.14 netbios-name-server 352
34.15 netbios-node-type 352
34.16 next-server 353
34.17 domain-name 354
34.18 bootfile 354
34.19 show ip dhcp server status 355
34.20 show ip dhcp server statistics 355
34.21 show ip dhcp server extend-option 356
34.22 show ip dhcp server pool 356
34.23 show ip dhcp server excluded-address 357
34.24 show ip dhcp server manual-binding 357
34.25 show ip dhcp server binding 358
34.26 clear ip dhcp server statistics 358
34.27 clear ip dhcp server binding 359

Chapter 35 DHCP Relay Commands 360

35.1 service dhcp relay 360
35.2 ip dhcp relay hops 360
35.3 ip dhcp relay time 361
35.4 ip helper-address 362
35.5 ip dhcp relay dynamic-circuit-id 362
35.6 ip dhcp relay dynamic-remote-id 364

35.7 ip dhcp relay information option 366
35.8 ip dhcp relay information strategy 366
35.9 ip dhcp relay information format 367
35.10 ip dhcp relay information circuit-id 368
35.11 ip dhcp relay information remote-id 369
35.12 ip dhcp relay information circuit-id-dynamic 369
35.13 ip dhcp relay information remote-id-dynamic 370
35.14 ip dhcp relay default-interface 371
35.15 ip dhcp relay vlan 372
35.16 show ip dhcp relay 372
35.17 show ip dhcp relay dynamic-option82 373
35.18 show ip dhcp relay information interface 373

Chapter 36 DHCP L2 Relay Commands 375

36.1 ip dhcp l2relay 375
36.2 ip dhcp l2relay vlan 375
36.3 ip dhcp l2relay dynamic-circuit-id 376
36.4 ip dhcp l2relay dynamic-remote-id 376
36.5 ip dhcp l2relay information option 377
36.6 ip dhcp l2relay information strategy 378
36.7 ip dhcp l2relay information format 379
36.8 ip dhcp l2relay information circuit-id 380
36.9 ip dhcp l2relay information remote-id 380
36.10 show ip dhcp l2relay 381
36.11 show ip dhcp l2relay interface 382
36.12 show ip dhcp l2relay dynamic-option82 382
36.13 show ip dhcp l2relay information interface 383

Chapter 37 QoS Commands 384

37.1 qos trust 384
37.2 qos port-priority 384
37.3 qos cos-map 385
37.4 qos dot1p-remap 386
37.5 qos dscp-map 387
37.6 qos dscp-remap 388
37.7 qos queue mode 389
37.8 show qos cos-map 390
37.9 show qos dot1p-remap interface 391

37.10 show qos dot1p-remap 391
37.11 show qos dscp-map interface 392
37.12 show qos dscp-map 393
37.13 show qos dscp-remap interface 393
37.14 show qos dscp-remap 394
37.15 show qos port-priority interface 394
37.16 show qos trust interface 395
37.17 show qos queue interface 395

Chapter 38 Bandwidth Control Commands 397

38.1 storm-control rate-mode 397
38.2 storm-control 398
38.3 storm-control exceed 399
38.4 storm-control recover 400
38.5 bandwidth 400
38.6 show storm-control 401
38.7 show bandwidth 402

Chapter 39 Voice VLAN Commands 403

39.1 voice vlan 403
39.2 voice vlan (interface) 403
39.3 voice vlan priority 404
39.4 voice vlan oui 405
39.5 show voice vlan 405
39.6 show voice vlan oui-table 406
39.7 show voice vlan interface 406

Chapter 40 Auto VoIP Commands 408

40.1 auto-voip 408
40.2 auto-voip (interface) 408
40.3 auto-voip dot1p 409
40.4 auto-voip untagged 410
40.5 auto-voip none 410
40.6 no auto-voip (interface) 411
40.7 auto-voip dscp 411
40.8 auto-voip data priority 412
40.9 show auto-voip 412

Chapter 41 Access Control Commands 414

41.1 user access-control ip-based enable 414
41.2 user access-control ip-based 414
41.3 user access-control mac-based enable 415
41.4 user access-control mac-based 416
41.5 user access-control port-based enable 417
41.6 user access-control port-based 417

Chapter 42 HTTP and HTTPS Commands 419

42.1 ip http server 419
42.2 ip http port 420
42.3 ip http max-users 420
42.4 ip http session timeout 421
42.5 ip http secure-server 422
42.6 ip http secure-port 422
42.7 ip http secure-protocol 423
42.8 ip http secure-ciphersuite 424
42.9 ip http secure-max-users 425
42.10 ip http secure-session timeout 426
42.11 ip http secure-server download certificate 426
42.12 ip http secure-server download key 427
42.13 show ip http configuration 428
42.14 show ip http secure-server 429

Chapter 43 SSH Commands 430

43.1 ip ssh server 430
43.2 ip ssh port 430
43.3 ip ssh version 431
43.4 ip ssh algorithm 432
43.5 ip ssh algorithm compatibility 432
43.6 ip ssh session-timeout 433
43.7 ip ssh max-client 434
43.8 ip ssh download 434
43.9 remove public-key 435
43.10 show ip ssh 436

Chapter 44 Telnet Commands 437

44.1 telnet 437

44.2 telnet enable 437
44.3 telnet port 438
44.4 show telnet-status 438

Chapter 45 Serial Port Commands 440

45.1 serial_port baud-rate 440

Chapter 46 Port Security Commands 441

46.1 mac address-table max-mac-count 441
46.2 show mac address-table max-mac-count 441

Chapter 47 Port Mirroring Commands 443

47.1 monitor session destination interface 443
47.2 monitor session source 444
47.3 show monitor session 445

Chapter 48 ACL Commands 447

48.1 access-list create 447
48.2 access-list resequence 447
48.3 access-list mac 448
48.4 access-list ip 450
48.5 access-list combined 452
48.6 access-list ipv6 454
48.7 access-list action 455
48.8 redirect 456
48.9 traffic 457
48.10 s-mirror 457
48.11 qos-remark 458
48.12 access bind 459
48.13 show access-list 460
48.14 show access-list bind 460
48.15 show access-list status 461
48.16 show access-list counter 461
48.17 clear access-list 462

Chapter 49 DHCPv4 Filter Commands 463

49.1 ip dhcp filter 463
49.2 ip dhcp filter (interface) 463
49.3 ip dhcp filter mac-verify 464

49.4 ip dhcp filter limit rate 465
49.5 ip dhcp filter decline rate 466
49.6 ip dhcp filter server permit-entry 466
49.7 show ip dhcp filter 467
49.8 show ip dhcp filter interface 468
49.9 show ip dhcp filter server permit-entry 468

Chapter 50 DHCPv6 Filter Commands 470

50.1 ipv6 dhcp filter 470
50.2 ipv6 dhcp filter (interface) 470
50.3 ipv6 dhcp filter limit rate 471
50.4 ipv6 dhcp filter decline rate 472
50.5 ipv6 dhcp filter server permit-entry 473
50.6 show ipv6 dhcp filter 474
50.7 show ipv6 dhcp filter interface 474
50.8 show ip dhcp filter server permit-entry 475

Chapter 51 Ethernet OAM Commands 476

51.1 ethernet-oam 476
51.2 ethernet-oam mode 476
51.3 ethernet-oam link-monitor symbol-period 477
51.4 ethernet-oam link-monitor frame 478
51.5 ethernet-oam link-monitor frame-period 479
51.6 ethernet-oam link-monitor frame-seconds 480
51.7 ethernet-oam remote-failure 481
51.8 ethernet-oam remote-loopback received-remote- loopback 482
51.9 ethernet-oam remote-loopback 483
51.10 clear ethernet-oam statistics 484
51.11 clear ethernet-oam event-log 484
51.12 show ethernet-oam configuration 485
51.13 show ethernet-oam event-log 486
51.14 show ethernet-oam statistics 486
51.15 show ethernet-oam status 487

Chapter 52 DLDP Commands (Only for Certain Devices) 488

52.1 dldp (global) 488
52.2 dldp interval 488
52.3 dldp shut-mode 489
52.4 dldp reset (global) 490

52.5 dldp(interface) 490
52.6 show dldp 491
52.7 show dldp interface 491

Chapter 53 SNMP Commands 493

53.1 snmp-server 493
53.2 snmp-server view 493
53.3 snmp-server group 494
53.4 snmp-server user 496
53.5 snmp-server community 497
53.6 snmp-server host 498
53.7 snmp-server engineID 500
53.8 snmp-server traps snmp 501
53.9 snmp-server traps 502
53.10 snmp-server traps ddm 503
53.11 snmp-server traps vlan 504
53.12 snmp-server traps security 505
53.13 snmp-server traps acl 506
53.14 snmp-server traps ip 506
53.15 snmp-server traps link-status 507
53.16 rmon history 508
53.17 rmon event 509
53.18 rmon alarm 510
53.19 rmon statistics 511
53.20 show snmp-server 512
53.21 show snmp-server view 512
53.22 show snmp-server group 513
53.23 show snmp-server user 513
53.24 show snmp-server community 514
53.25 show snmp-server host 514
53.26 show snmp-server engineID 515
53.27 show rmon history 515
53.28 show rmon event 516
53.29 show rmon alarm 516
53.30 show rmon statistics 517

Chapter 54 ND Detection Commands 518

54.1 ipv6 nd detection 518

54.2 ipv6 nd detection vlan 518
54.3 ipv6 nd detection vlan logging 519
54.4 ipv6 nd detection trust 519
54.5 show ipv6 nd detection 520
54.6 show ipv6 nd detection interface 520
54.7 show ipv6 nd detection statistics 521
54.8 show ipv6 nd detection vlan 522

Chapter 55 System Log Commands 523

55.1 logging buffer 523
55.2 logging buffer level 523
55.3 logging file flash 524
55.4 logging file flash frequency 525
55.5 logging file flash level 526
55.6 logging host index 526
55.7 logging console 527
55.8 logging console level 528
55.9 logging monitor 529
55.10 logging monitor level 529
55.11 clear logging 530
55.12 show logging local-config 531
55.13 show logging loghost 531
55.14 show logging buffer 532
55.15 show logging flash 532

Chapter 56 ERPS Commands 534

56.1 erps ring 534
56.2 control-vlan 534
56.3 description 535
56.4 guard-timer 536
56.5 wtr-timer 536
56.6 holdoff-timer 537
56.7 protected-instance 538
56.8 raps-mel 538
56.9 revertive 539
56.10 sub-ring 540
56.11 tc-notify erps 540
56.12 tc-protection interval 541

56.13 tc-protection threshold 541
56.14 version 542
56.15 virtual-channel 543
56.16 erps ring rpl 543
56.17 erps ring protect-switch 544
56.18 no erps ring ringid description 545
56.19 no erps ring ringid raps-mel 545
56.20 no erps ring ringid version 546
56.21 show erps ring 546
56.22 show erps statistics 547

Chapter 57 IS-IS Configuration Commands 548

57.1 router isis 548
57.2 area-password 549
57.3 domain-password 549
57.4 graceful-restart 550
57.5 hostname 551
57.6 is-type 552
57.7 log-adjacency-changes 553
57.8 lsp-gen-interval 553
57.9 lsp-mtu 554
57.10 lsp-refresh-interval 555
57.11 max-lsp-lifetime 555
57.12 metric-style 556
57.13 net 557
57.14 purge-originator 557
57.15 set-attached-bit 558
57.16 set-overload-bit 559
57.17 spf interval 559
57.18 topology 560
57.19 clear isis neighbor 561
57.20 redistribute 561
57.21 distance 562
57.22 ip router isis 563
57.23 ipv6 router isis 564
57.24 isis bfd 564
57.25 isis circuit-type 565
57.26 isis csnp-interval 566

57.27 isis hello-interval 566
57.28 isis hello-multiplier 567
57.29 isis metric 568
57.30 isis network point-to-point 568
57.31 isis passive 569
57.32 isis password-key 570
57.33 isis priority 570
57.34 topology 571
57.35 isis three-way-handshake 572
57.36 show isis database 573
57.37 show isis graceful-restart 573
57.38 show isis hostname 574
57.39 show isis neighbor 574
57.40 show isis route 575
57.41 show isis summary 575
57.42 show isis interface 576
57.43 show isis topology 576

Chapter 58 RIP Configuration Commands 578

58.1 router rip 578
58.2 network 578
58.3 version 579
58.4 timer basic 580
58.5 distance 581
58.6 auto-summary 581
58.7 default-metric 582
58.8 redistribute 582
58.9 allow-ecmp 583
58.10 default-information originate 584
58.11 neighbor 584
58.12 passive-interface 585
58.13 ip rip authentication mode 585
58.14 ip rip authentication string 586
58.15 ip rip authentication key-chain 587
58.16 ip rip receive version 588
58.17 ip rip send version 588
58.18 ip rip split-horizon 589
58.19 ip rip v2-broadcast 590

58.20 show ip rip 590
58.21 show ip rip status 591
58.22 clear ip rip 591

Chapter 59 RIPng Configuration Commands 593

59.1 router ripng 593
59.2 ipv6 rip enable 594
59.3 timer basic 594
59.4 default-metric 595
59.5 redistribute 596
59.6 allow-ecmp 596
59.7 default-information originate 597
59.8 passive-interface 597
59.9 ip rip split-horizon 598
59.10 show ipv6 rip 599
59.11 show ipv6 rip status 599
59.12 clear ipv6 rip 600

Chapter 60 OSPF Configuration Commands 601

60.1 router ospf 601
60.2 router-id 602
60.3 network 602
60.4 maximum-paths 603
60.5 redistribute 604
60.6 default-metric 605
60.7 default-metric 605
60.8 auto-cost 606
60.9 distance 607
60.10 timers throttle spf 608
60.11 compatible rfc 1583 608
60.12 area stub 609
60.13 area nssa 610
60.14 area default-cost 611
60.15 area range 611
60.16 area authentication 612
60.17 area virtual-link 613
60.18 area virtual-link authentication 614
60.19 area virtual-link authentication-key 615

60.20 area virtual-link message-digest-key 616
60.21 capability opaque 617
60.22 graceful-restart 617
60.23 graceful-restart grace-period 618
60.24 graceful-restart helper 619
60.25 graceful-restart helper planned-only 619
60.26 graceful-restart helper strict-lsa-checking 620
60.27 ip ospf cost 621
60.28 ip ospf retransmit-interval 621
60.29 ip ospf transmit-delay 622
60.30 ip ospf priority 623
60.31 ip ospf hello-interval 623
60.32 ip ospf dead-interval 624
60.33 ip ospf authentication 625
60.34 ip ospf authentication-key 625
60.35 ip ospf message-digest-key 626
60.36 ip ospf network 627
60.37 ip ospf mtu-ignore 627
60.38 ip ospf passive 628
60.39 clear ip ospf 629
60.40 show ip ospf 629
60.41 show ip ospf database 630
60.42 show ip ospf interface 630
60.43 show ip ospf neighbor 631
60.44 show ip ospf border-routers 632
60.45 show ip ospf route 632
60.46 show ip ospf [process-id] graceful-restart helper 633

Chapter 61 Service Port Profile Configuration Commands 634

61.1 ont-srvport-profile gpon 634
61.2 show ont-srvport-profile gpon 635
61.3 service-port 636
61.4 show ont-srvport-profile gpon bound-info 637

Chapter 62 IPv4 IMPB Commands 638

62.1 ip source binding 638
62.2 no ip source binding interface 639
62.3 ip dhcp snooping 640

62.4 ip dhcp snooping vlan 640
62.5 ip dhcp snooping max-entries 641
62.6 ip dhcp snooping trust 642
62.7 show ip source binding 642
62.8 show ip dhcp snooping 643
62.9 show ip dhcp snooping interface 643

Chapter 63 IPv6 IMPB Commands 645

63.1 ipv6 source binding 645
63.2 no ipv6 source binding interface 646
63.3 ipv6 dhcp snooping 647
63.4 ipv6 dhcp snooping vlan 647
63.5 ipv6 dhcp snooping max-entries 648
63.6 ipv6 nd snooping 649
63.7 ipv6 nd snooping vlan 649
63.8 ipv6 nd snooping max-entries 650
63.9 show ipv6 source binding 651
63.10 show ipv6 dhcp snooping 651
63.11 show ipv6 dhcp snooping interface 652
63.12 show ipv6 nd snooping 653
63.13 show ipv6 nd snooping interface 653

Chapter 64 DoS Defend Commands 655

64.1 ip dos-prevent 655
64.2 ip dos-prevent type 655
64.3 show ip dos-prevent 657

Chapter 65 ARP Inspection Commands 659

65.1 ip arp inspection 659
65.2 ip arp inspection validate 659
65.3 ip arp inspection vlan 660
65.4 ip arp inspection vlan logging 661
65.5 ip arp inspection trust 662
65.6 ip arp inspection limit-rate 662
65.7 ip arp inspection burst-interval 663
65.8 ip arp inspection recover 664
65.9 ip arp inspection exceed 664
65.10 show ip arp inspection 665
65.11 show ip arp inspection interface 666

65.12 show ip arp inspection vlan 666
65.13 show ip arp inspection statistics 667
65.14 clear ip arp inspection statistics 667

Chapter 66 ARP Scan Commands 669

66.1 ip arp scan 669
66.2 ip arp scan apply 669
66.3 show ip arp scan 670

Chapter 67 SDM Template Commands 672

67.1 sdm prefer 672
67.2 show sdm prefer 673

Chapter 68 IPv6 Neighbor Commands 675

68.1 show ipv6 neighbors 675
68.2 clear ipv6 neighbors 675

Chapter 69 File System Configuration Commands 677

69.1 copy 677
69.2 cd 677
69.3 dir 678
69.4 pwd 678
69.5 rename 679
69.6 delete 679
69.7 ftp 680
69.8 open 680
69.9 put 681
69.10 get 682
69.11 close 682

Chapter 70 AAA Commands 683

70.1 tacacs-server host 683
70.2 show tacacs-server 684
70.3 radius-server host 685
70.4 show radius-server 687
70.5 show radius-server certificate 687
70.6 aaa group 688
70.7 server 688
70.8 show aaa group 689

70.9 aaa authentication login 690
70.10 aaa authentication enable 691
70.11 aaa authentication dot1x default 692
70.12 aaa accounting dot1x default 692
70.13 show aaa authentication 693
70.14 show aaa accounting 694
70.15 line telnet 694
70.16 login authentication (telnet) 695
70.17 line ssh 695
70.18 login authentication (ssh) 696
70.19 line console 697
70.20 login authentication (console) 697
70.21 enable authentication (telnet) 698
70.22 enable authentication (ssh) 699
70.23 enable authentication (console) 699
70.24 ip http login authentication 700
70.25 ip http enable authentication 701
70.26 show aaa global 701
70.27 enable admin password 702
70.28 enable admin secret 703
70.29 enable-admin 704

Chapter 71 IEEE 802.1x Commands 706

71.1 dot1x system-auth-control 706
71.2 dot1x handshake 707
71.3 dot1x auth-protocol 707
71.4 dot1x vlan-assignment 708
71.5 dot1x accounting 709
71.6 dot1x mab 710
71.7 dot1x guest-vlan 710
71.8 dot1x timeout quiet-period 711
71.9 dot1x timeout supp-timeout 712
71.10 dot1x max- req 713
71.11 dot1x 713
71.12 dot1x port-control 714
71.13 dot1x port-method 715
71.14 dot1x auth-init 716
71.15 dot1x auth-reauth 716

71.16 show dot1x global 717
71.17 show dot1x interface 718
71.18 show dot1x auth-state interface 718

Chapter 72 Board Management Commands 720

72.1 show board 720
72.2 board add 721
72.3 board auto-load 721
72.4 board delete 722
72.5 board load 723
72.6 board lock 723
72.7 board switch-over 724

Preface

This Guide is intended for network administrator to provide referenced information about CLI (Command Line Interface). The device mentioned in this Guide stands for DeltaStream GPON Optical Line Terminal without any explanation. Some models featured in this guide may be unavailable in your country or region. For local sales information, visit https://www.tp-link.com.

Chapter 1 Using the CLI

1.1 Accessing the CLI

You can log on to the device and access the CLI by the following three methods:

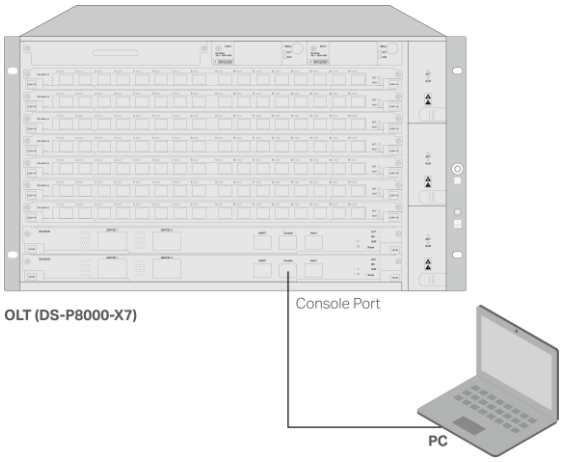
1. Logon Via the Console Port.
2. Logon By Telnet.
3. Logon By SSH.

Note: We take DS-P8000-X7 as an example of OLT devices in the following figures.

1.1.1 Via the Console Port

Take the following steps to log on to the device via the Console Port.

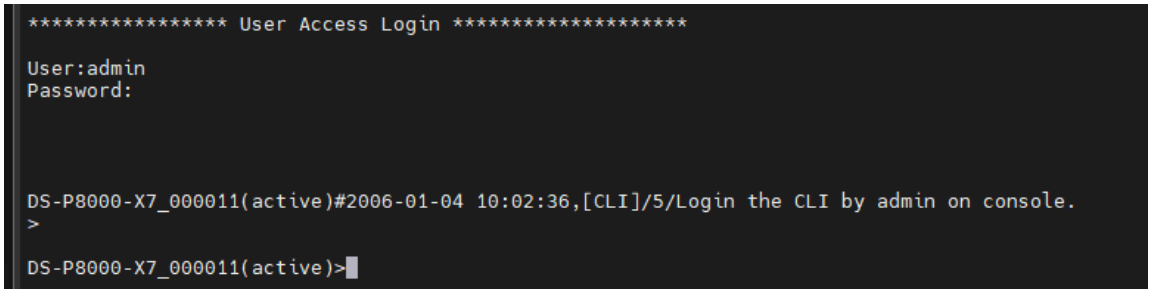
1. Connect the Console port of OLT to the management PC using an RJ45 console cable.



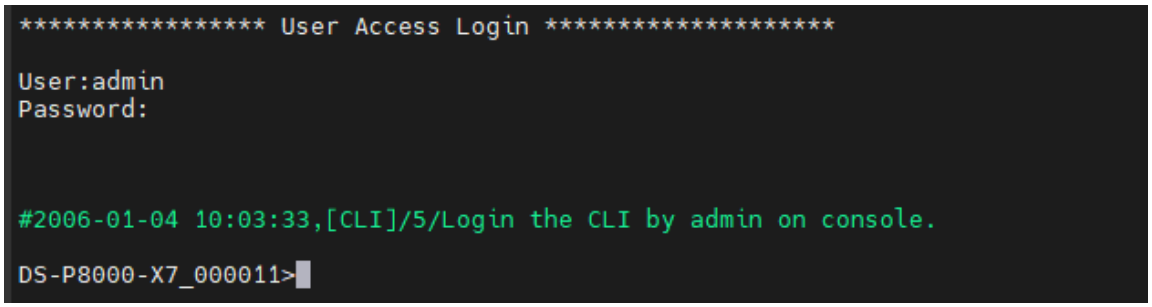
2. Start the terminal emulation program (such as the Hyper Terminal) on the PC and configure the terminal emulation program as follows:
   - Baud rate: 38400 bps
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Flow control: none

3. Type the Username and Password in the Hyper Terminal window. Press **Enter** in the main window and "Device>" will appear indicating that you have successfully logged in to the device and you can use the CLI now.

   Example for main control board:



   Example for standby control board:



Note: The first time you log in, set the password to better protect your network and devices.

1.1.2 Logon by Telnet

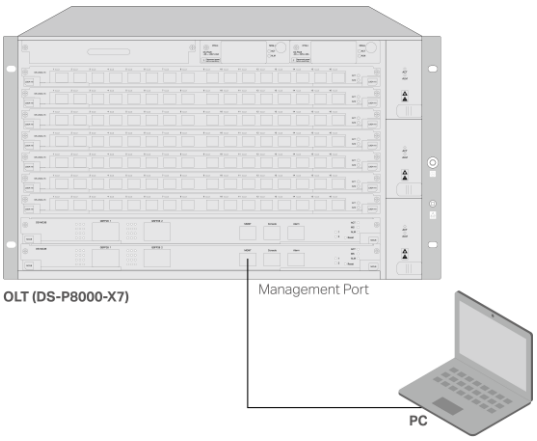
Note: The Telnet feature is disabled by default. Before you log on the device by Telnet, you need to enable the Telnet feature using the Web UI, via the Console Port.

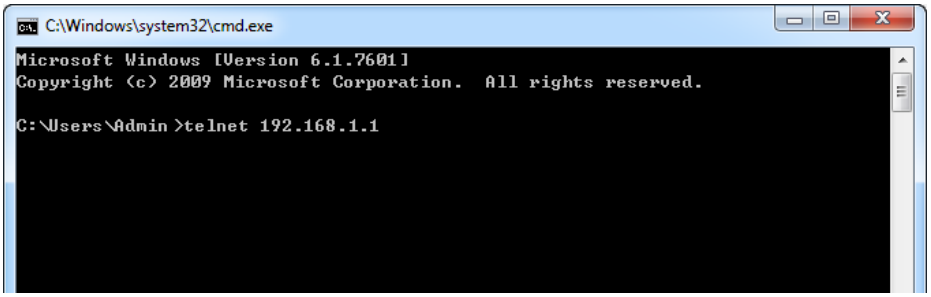
To log on to the device via a Telnet connection, please take the following steps:

1. Connect the OLT to the management PC. Choose from the following options:

   - **Via the MGMT Port**

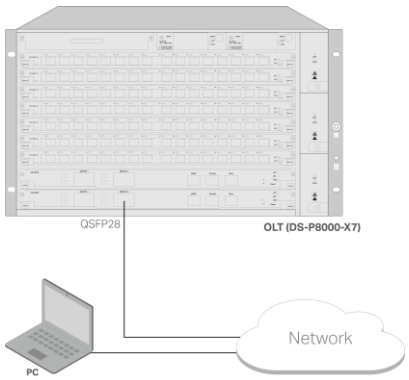
   Connect the MGMT port of OLT to the management PC using an Ethernet cable. Set the IP address of the PC as 192.168.1.x/24 (x is a number between 2 and 254). Open the terminal on the PC. Then type in "telnet 192.168.1.1" and press **Enter**.

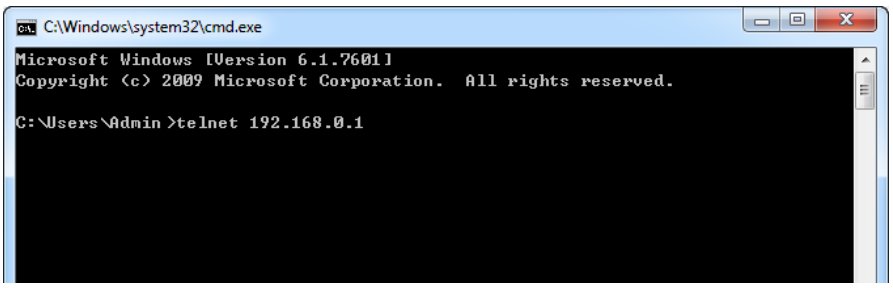




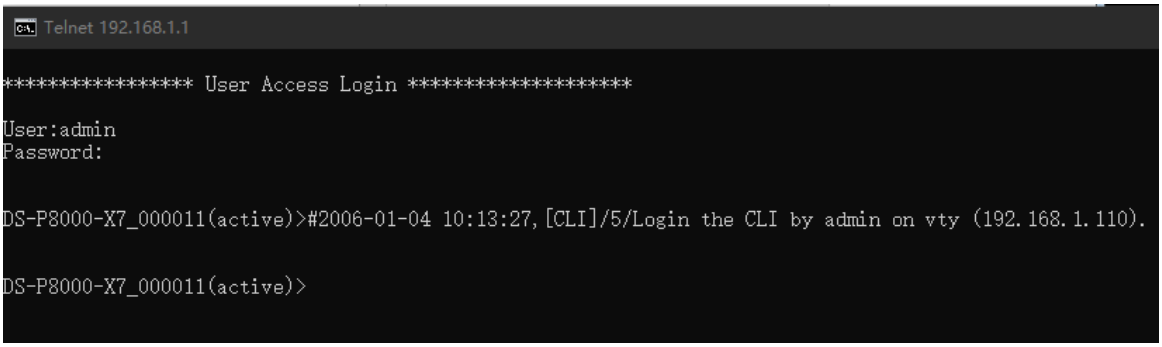
- **Via the QSFP28/ SFP+/GE Port**

Make sure your PC has network access to the QSFP28/SFP+/GE port of OLT. Set the IP address of the PC as 192.168.0.x/24 (x is a number between 2 and 254). Open the terminal on the PC. Then type in “telnet 192.168.0.1” and press **Enter**.





2. Enter the username and password and you will enter User EXEC Mode. Enter **enable** and you will enter Privileged EXEC Mode.



Note: The first time you log in, set the password to better protect your network and devices.

1.1.3 Logon by SSH

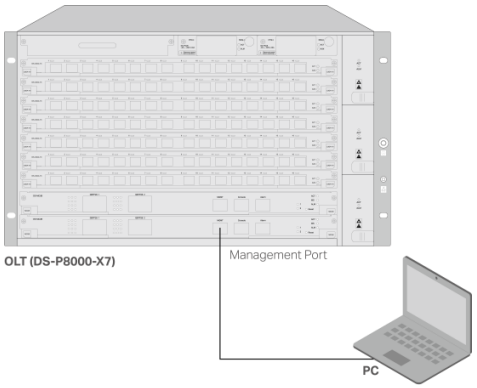
Note: The SSH feature is disabled by default. Before you log on the device by SSH, you need to enable the SSH feature using the Web UI, via the Console Port or using Telnet.

To log on to the device via an SSH connection, please take the following steps:

1. Connect the OLT to the management PC. Choose from the following options:

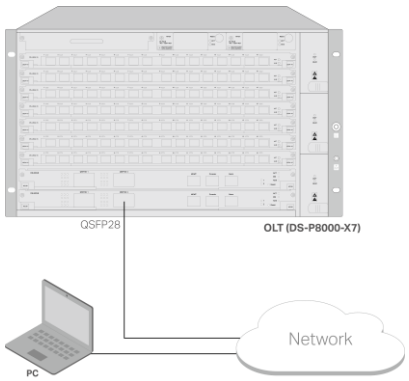
   - **Via the MGMT Port**

     Connect the MGMT port of OLT to the management PC using an Ethernet cable. Set the IP address of the PC as 192.168.1.x/24 (x is a number between 2 and 254).



   - **Via the QSFP28/SFP+/GE Port**

     Make sure your PC has network access to the QSFP28/SFP+/GE port of OLT. Set the IP address of the PC as 192.168.0.x/24 (x is a number between 2 and 254).

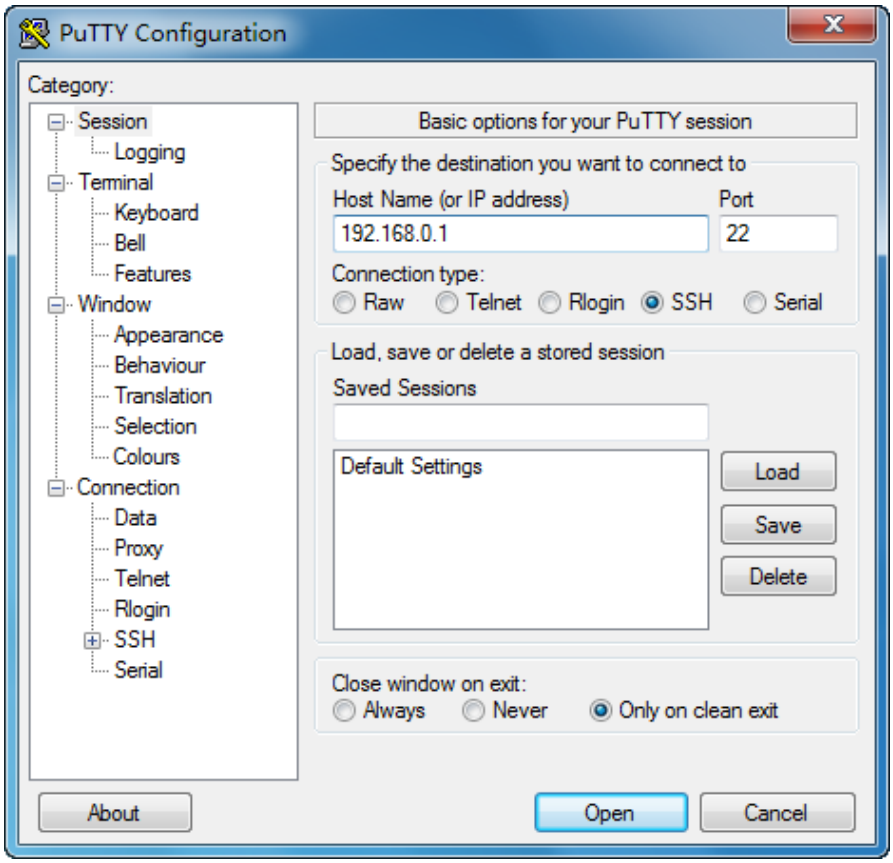


2. To log on by SSH, a Putty client software is recommended. There are two authentication modes to set up an SSH connection:

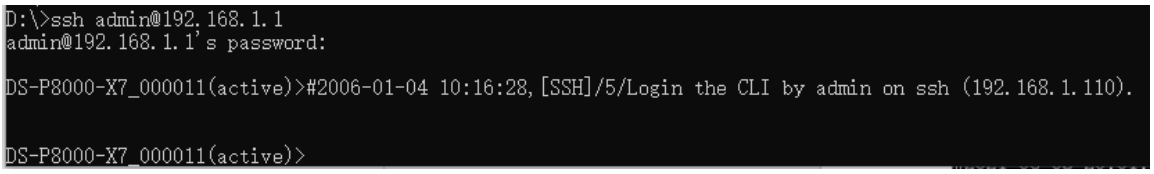
   - **Password Authentication Mode**

   It requires username and password, which are created when you first log in.

   Open the software to log on to the interface of PuTTY. Enter the IP address of the device into **Host Name** field (192.168.1.1 for MGMT Port; 192.168.0.1 for SFP+/GE Port). Keep the default value 22 in the **Port** field. Select **SSH** as the Connection type.



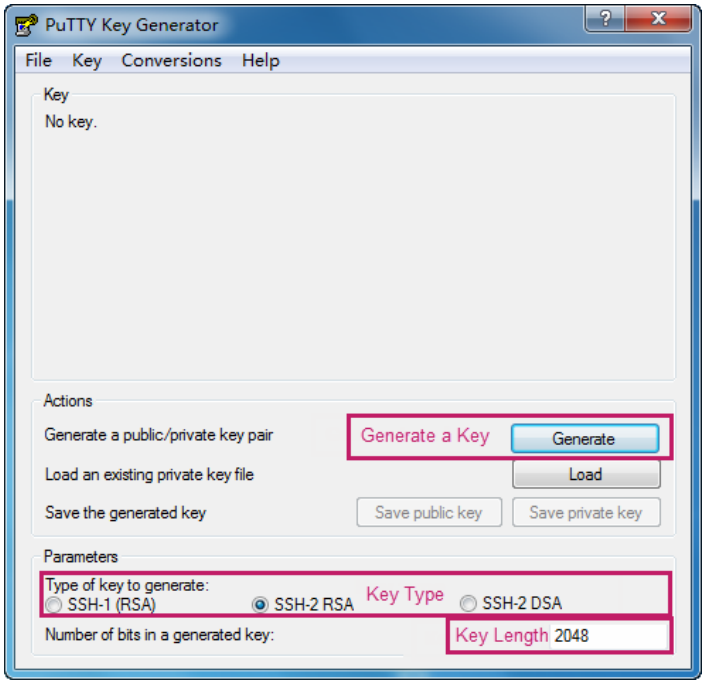
Click **Open** to log on to the device. Enter the username and password and you will enter User EXEC Mode. Enter **enable** and you will enter Privileged EXEC Mode.



Note: The first time you log in, set the password to better protect your network and devices.

- **Key Authentication Mode**

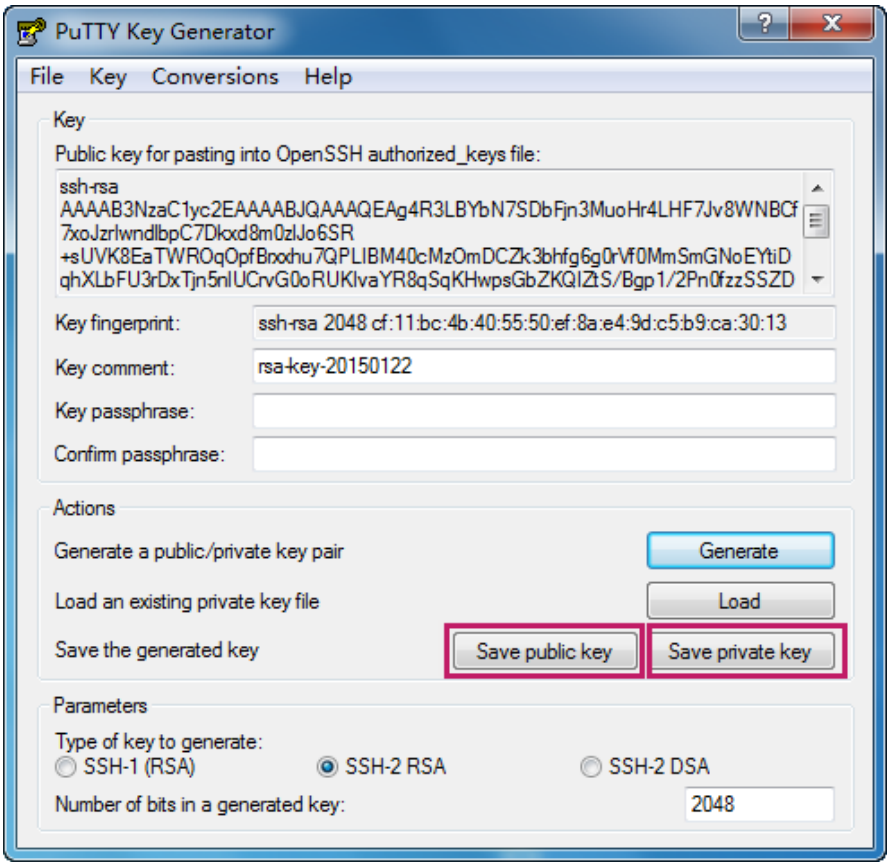
It requires a public key for the device and a private key for the SSH client software. You can generate the public key and the private key through Putty Key Generator. Select the key type and key length, and generate SSH key.



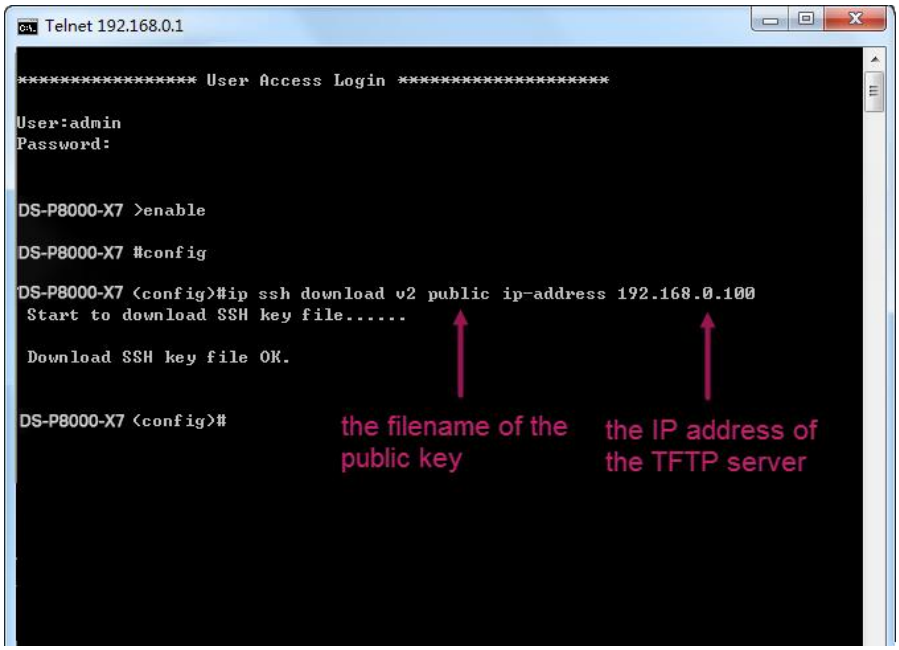
Note:

1. The key length is in the range of 512 to 3072 bits.
2. During the key generation, randomly moving the mouse quickly can accelerate the process.

After the key is successfully generated, please save the public key and private key to a TFTP server.



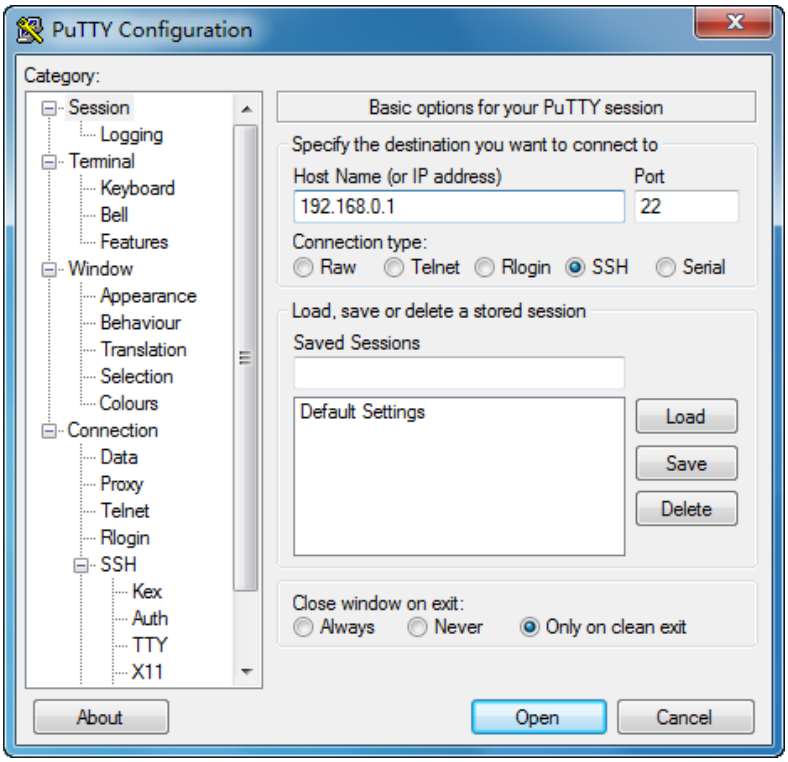
Log on to the device via the Console Port or using Telnet to download the public key file from the TFTP server, as the following figure shows:



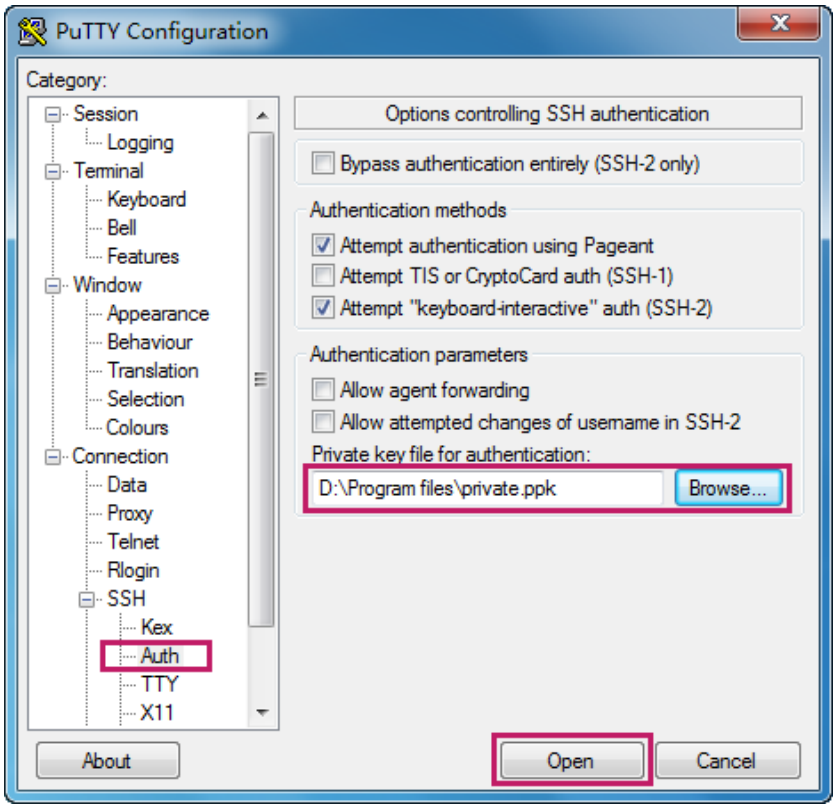
Note:

3. The key type should accord with the type of the key file.
4. The SSH key downloading can not be interrupted.

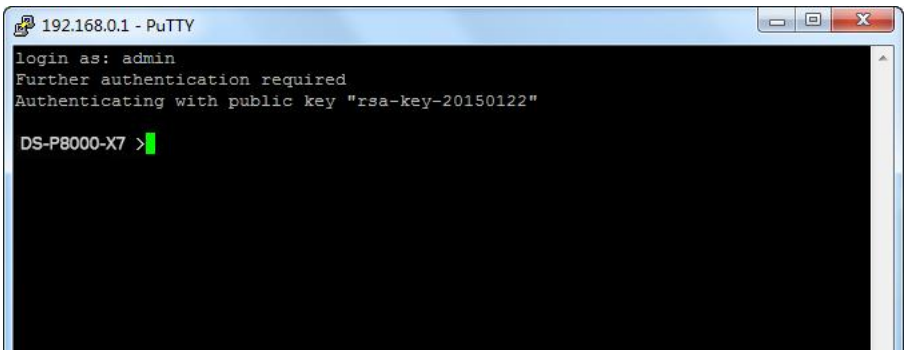
After the public key is downloaded, please log on to the interface of PuTTY and enter the IP address for login (192.168.1.1 for MGMT Port; 192.168.0.1 for SFP+/GE Port).



Go to **SSH** > **Auth**. Click **Browse** to download the private key file to the SSH client software and click **Open**.



After successful authentication, enter the user name. If you log on to the device without entering password, it indicates that the key has been successfully downloaded.



1.2 CLI Command Modes

The CLI is divided into different command modes: User EXEC Mode, Privileged EXEC Mode, Global Configuration Mode, Interface Configuration Mode and VLAN Configuration Mode. Interface Configuration Mode can also be divided into Interface Ethernet, Interface link-aggregation and some other modes.

The following table gives detailed information about the Accessing path, Prompt of the mode and how to exit the current mode and access the next mode.

Mode	Accessing Path	Prompt	Logout or Access the next mode
User EXEC Mode	Primary mode once it is connected with the device.	**Device>**	Use the **exit** command to disconnect the device. Use the **enable** command to access Privileged EXEC mode.
Privileged EXEC Mode	Use the **enable** command to enter this mode from User EXEC mode.	**Device #**	Enter the **exit** command to return to User EXEC mode. Enter **configure** command to access Global Configuration mode.
Global Configuration Mode	Use the **configure** command to enter this mode from Privileged EXEC mode.	**Device (config)#**	Use the **exit** or the **end** command or press **Ctrl+Z** to return to Privileged EXEC mode. Use the **interface gigabitEthernet** *port* or **interface range gigabitEthernet** *port-list* command to access interface Configuration mode. Use the **vlan** *vlan-list* to access VLAN Configuration mode.

Mode	Accessing Path	Prompt	Logout or Access the next mode
Interface Configuration Mode	Layer 2 Interface: Use the **interface gigabitEthernet** *port*, **interface port-channel** *port-channel-id* or **interface range gigabitEthernet** *port-list* command to enter this mode from Global Configuration mode.	**Device (config-if)#** or **Device (config-if-range)#**	Use the **end** command or press **Ctrl+Z** to return to Privileged EXEC mode. Enter the **exit** or the **#** command to return to Global Configuration mode. A port number must be specified in the **interface** command.
Interface Configuration Mode	Layer 3 Interface: Use the **no switchport** command to enter Routed Port mode from Interface Configuration mode. Use the **interface vlan** *vlan-id* command to enter VLAN Interface mode from Global Configuration mode. Use the **interface loopback** *id* command to enter Loopback Interface mode from Global Configuration mode.	**Device (config-if)#** or **Device (config-if-range)#**	Use the **switchport** command to switch to the Layer 2 interface mode. Use the **end** command or press **Ctrl+Z** to return to Privileged EXEC mode. Enter the **exit** or the **#** command to return to Global Configuration mode.
VLAN Configuration Mode	Use the **vlan** *vlan-list* command to enter this mode from Global Configuration mode.	**Device (config-vlan)#**	Use the **end** command or press **Ctrl+Z** to return to Privileged EXEC mode. Enter the **exit** command or the # command to return to Global configuration mode.

Note:

1. The user is automatically in User EXEC Mode after the connection between the PC and the

device is established by a Telnet/SSH connection.

2. Each command mode has its own set of specific commands. To configure some commands, you should access the corresponding command mode firstly.

    - **Global Configuration Mode**: In this mode, global commands are provided, such as the Spanning Tree, Schedule Mode and so on.
    - **Interface Configuration Mode**: In this mode, users can configure one or several ports, different ports corresponds to different commands

        a). Interface gigabitEthernet / hundred-gigabitEthernet / twentyFive-gigabitEthernet / gpon / xgspon: Configure parameters for a gigabitEthernet / hundred-gigabitEthernet / twentyFive-gigabitEthernet / gpon / xgspon port.

        b). Interface range gigabitEthernet/ hundred-gigabitEthernet / twentyFive-gigabitEthernet / gpon / xgspon: Configure parameters for several gigabitEthernet / hundred-gigabitEthernet / twentyFive-gigabitEthernet / gpon / xgspon ports.

        c). Interface link-aggregation: Configure parameters for a link-aggregation, such as broadcast storm.

        d). Interface range link-aggregation: Configure parameters for multi-trunks.

        e). Interface vlan: Configure parameters for the vlan-port.

    - **VLAN Configuration Mode**: In this mode, users can create a VLAN and add a specified port to the VLAN.

3. Some commands are global, that means they can be performed in all modes:

    - **show**: Display all information of device, for example: statistic information, port information, VLAN information.
    - **history**: Display the commands history.

4. The CLI prompt of the active main control board is prefixed with "(active)", while the standby control board does not.

1.3 Privilege Restrictions

This device's security is divided into four privilege levels: User level, Power User level, Operator level and Admin level. You can define username and password pairs, and assign a specific privilege level to each pair. Different privilege levels have access to specified commands, which is illustrated in the **Privilege Requirement** in each command. For details about how to

configure usename and password pairs, please refer to user name (password) and user name (secret).

Users can enter Privileged EXEC mode from User EXEC mode by using the **enable** command.By default, no password is needed. In Global Configuration Mode, you can configure password for Admin level by **enable password** command. Once password is configured, you are required to enter it to access Privileged EXEC mode.

1.4 Conventions

1.4.1 Format Conventions

The following conventions are used in this Guide:

- Items in square brackets [ ] are optional
- Items in braces { } are required
- Alternative items are grouped in braces and separated by vertical bars. For example: **speed** {10 | 100 | 1000 }
- Bold indicates an unalterable keyword. For example: **show logging**
- Normal Font indicates a constant (several options are enumerated and only one can be selected). For example: **mode** {dynamic | static | permanent}
- Italic Font indicates a variable (an actual value must be assigned). For example: **bridge aging-time** *aging-time*

1.4.2 Special Characters

You should pay attentions to the description below if the variable is a character string:

- These six characters " < > , \ & cannot be input.
- If a blank is contained in a character string, single or double quotation marks should be used, for example 'hello world', "hello world", and the words in the quotation marks will be identified as a string. Otherwise, the words will be identified as several strings.

1.4.3 Parameter Format

Some parameters must be entered in special formats which are shown as follows:

- MAC address must be entered in the format of xx:xx:xx:xx:xx:xx.

- One or several values can be typed for a port-list or a vlan-list using comma to separate. Use a hyphen to designate a range of values, for instance, 1/0/1, 1/0/3-5, 1/0/7 indicates choosing port 1/0/1, 1/0/3, 1/0/4, 1/0/5, 1/0/7.

Chapter 2 User Interface

2.1 enable

Description

The **enable** command is used to access Privileged EXEC Mode from User EXEC Mode.

Syntax

enable

Command Mode

User EXEC Mode

Privilege Requirement

None.

Example

If you have set the password to access Privileged EXEC Mode from User EXEC Mode:

```
Device>enable
Enter password:
Device#
```

2.2 service password-encryption

Description

The **service password-encryption** command is used to encrypt the password when the password is defined or when the configuration is written, using the symmetric encryption algorithm. Encryption prevents the password from being readable in the configuration file. To disable the global encryption function, please use **no service password-encryption** command.

Syntax

service password-encryption

no service password-encryption

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the global encryption function:

```
Device(config)# service password-encryption
```

2.3 enable password

Description

The **enable password** command is used to set or change the password for users to access Privileged EXEC Mode from User EXEC Mode. To remove the password, please use **no enable password** command. This command uses the symmetric encryption.

Syntax

enable password { [0] *password* | 7 *encrypted-password*}

no enable password

Parameter

0 —— Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password —— A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. By default, it is empty.

7 —— Indicates a symmetric encrypted password with fixed length will follow.

encrypted-password —— A symmetric encrypted password with fixed length, which you can copy from another Device's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If the password you configured here is unencrypted and the global encryption function is enabled in service password-encryption, the password in the configuration file will be displayed in the symmetric encrypted form.

If both the **enable password** and **enable secret** are defined, only the latest configured password will take effect.

Example

Set the super password as "admin" and unencrypted to access Privileged EXEC Mode from User EXEC Mode:

Device(config)#enable password 0 admin

2.4 enable secret

Description

The **enable secret** command is used to set a secret password, which is using an MD5 encryption algorithm, for users to access Privileged EXEC Mode from User EXEC Mode. To return to the default configuration, please use **no enable secret** command. This command uses the MD5 encryption.

Syntax

enable secret { [0] *password* **|** 5 *encrypted-password*}

no enable secret

Parameter

0 —— Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password —— A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. By default, it is empty. The password in the configuration file will be displayed in the MD5 encrypted form.

5 —— Indicates an MD5 encrypted password with fixed length will follow.

encrypted-password —— An MD5 encrypted password with fixed length, which you can copy from another Device's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **enable password** and **enable secret** are defined, only the latest configured password will take effect.

Example

Set the secret password as “admin” and unencrypted to access Privileged EXEC Mode from User EXEC Mode. The password will be displayed in the encrypted form.

Device(config)#enable secret 0 admin

2.5 configure

Description

The **configure** command is used to access Global Configuration Mode from Privileged EXEC Mode.

Syntax

configure

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Access Global Configuration Mode from Privileged EXEC Mode:

Device# configure
Device (config)#

2.6 exit

Description

The **exit** command is used to return to the previous Mode from the current Mode.

Syntax

exit

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Return to Global Configuration Mode from Interface Configuration Mode, and then return to Privileged EXEC Mode:

```
Device (config-if)# exit
Device (config)#exit
Device#
```

2.7 end

Description

The **end** command is used to return to Privileged EXEC Mode.

Syntax

end

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Return to Privileged EXEC Mode from Interface Configuration Mode:

```
Device (config-if)#end
Device #
```

2.8 clipaging

Description

The **clipaging** command is used to enable the pause function for the screen display. If you want to display all the related information of the Device at once when using the show command, please use **no clipaging** command.

Syntax

clipaging

no clipaging

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Disable the pause function for the screen display:

```
Device (config)#no clipaging
```

2.9 history

Description

The **history** command is used to show the latest 20 commands you entered in the current mode since the Device is powered.

Syntax

history

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

None.

Example

Show the commands you have entered in the current mode:

```
Device (config)# history

    1 history
```

2.10 history clear

Description

The **history clear** command is used to clear the commands you have entered in the current mode; therefore, these commands will not be shown next time you use the **history** command.

Syntax

history clear

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the commands you have entered in the current mode:

```
Device (config)#history clear
```

Chapter 3 User Management Commands

User Management commands are used to manage the user's logging information by Web, Telnet or SSH, so as to protect the settings of the Device from being randomly changed.

3.1 user name (password)

Description

The **user name** command is used to add a new user or modify the existed users' information. To delete the existed users, please use **no user name** command. This command uses the symmetric encryption.

Syntax

user name *name* [privilege admin | operator | power_user | user] **password** { [0] *password* | 6 *encrypted-password* | 7 *encrypted-password*}

no user name *name*

Parameter

name ——Type a name for users' login. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.

admin | operator | power_user | user —— Access level. "admin" means that you can edit, modify and view all the settings of different functions. "operator" means that you can edit, modify and view most of the settings of different functions. "power-user" means that you can edit, modify and view some of the settings of different functions. "user" means that you can only view some of the settings of different functions without the right to edit or modify. It is "admin" by default. For more details about privilege restrictions, please refer to the **Privilege Requirement** part in each command.

0 —— Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password —— Users' login password, a string with 10-64 digits, alphanumeric characters (case-sensitive) and symbols. No spaces are allowed. Allowed symbols: !"#$%&'()*+,-.\/:;<>=@[]^_`{}|~

6 —— Indicates a custom encrypted password with fixed length will follow.

7 —— Indicates a symmetric encrypted password with fixed length will follow.

encrypted-password—— A custom/symmetric encrypted password with fixed length, which you can copy from another Device's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If the password you configured here is unencrypted and the global encryption function is enabled in service password-encryption, the password in the configuration file will be displayed in the symmetric encrypted form.

If both the **user name (password)** and **user name (secret)** are defined, only the latest configured password will take effect.

Example

Add and enable a new admin user named "tplink", of which the password is "admin" and unencrypted:

```
Device(config)#user name tplink privilege admin password 0 admin
```

3.2 user name (secret)

Description

The **user name** command is used to add a new user or modify the existed users' information. To delete the existed users, please use **no user name** command. This command uses the MD5 encryption.

Syntax

user name *name* [privilege admin | operator | power_user | user] **secret** { [0] *password* | 4 *encrypted-password* | 5 *encrypted-password* | 8 *encrypted-password* | 9 *encrypted-password*}

no user name *name*

Parameter

name ——Type a name for users' login. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.

admin | operator | power_user | user —— Access level. “admin” means that you can edit, modify and view all the settings of different functions. “operator” means that you can edit, modify and view most of the settings of different functions. “power-user” means that you can edit, modify and view some of the settings of different functions. “user” means that you can only view some of the settings of different functions without the right to edit or modify. It is “admin” by default.

0 —— Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password ——Users' login password, a string with 6–31 alphanumeric characters (case-sensitive) and symbols. No spaces are allowed.

4 —— Indicates an SHA256 encrypted password with fixed length will follow.

5 —— Indicates an MD5 encrypted password with fixed length will follow.

8 ——Indicates an PBKDF2 encrypted password with fixed length will follow.

9 ——Indicates a SCRYPT encrypted password with fixed length will follow.

encrypted-password —— An/A SHA256/MD5/SCRYPT/PBKDF2 encrypted password with fixed length, which you can copy from another device's configuration file.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **user name (password)** and **user name (secret)** are defined, only the latest configured password will take effect.

Example

Add and enable a new admin user named “tplink”, of which the password is “admin”. The password will be displayed in the encrypted form.

Device (config)#user name tplink **privilege** admin **secret** 0 admin

3.3 show user account-list

Description

The **show user account-list** command is used to display the information of the current users.

Syntax

show user account-list

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the current users:

```
Device (config)# show user account-list
```

3.4 show user configuration

Description

The **show user configuration** command is used to display the security configuration information of the users, including access-control, max-number and the idle-timeout, etc.

Syntax

show user configuration

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration information of the users:

```
Device (config)# show user configuration
```

Chapter 4 Management Port Configuration Commands

4.1 description

Description

The **description** command is used to specify management interface description.

Syntax

description *description*

Parameter

description—— Up to 16 characters describing this interface.

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify management interface description:

```
Device (config-if)# description desc1
```

4.2 ip

Description

The **ip** command is used to configure interface address.

Syntax

ip {address *address mask* [gateway *gateway* | secondary] | address-alloc {bootp | dhcp} | dhcp option12 *hostname* }

Parameter

address—— Specify the static IP address.

mask—— Specify the IP subnet mask.

gateway—— Specify the gateway.

secondary—— Secondary IP address.

bootp—— Set IP address by bootp.

dhcp—— Set IP address by dhcp.

hostname—— Host name string.

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure interface address:

```
Device (config-if)# ip address 192.168.0.1 255.255.255.0 gateway 10.0.0.1
```

4.3 ipv6

Description

The **ipv6** command is for the IPv6 interface subcommands.

Syntax

Ipv6 {address {*address* [eui-64] | *global-address* [eui-64] | autoconfig | dhcp} | enable | gateway [*gateway*] }

Parameter

address—— IPv6 link-local address.

global-address—— Config global IPv6 address manully.

autoconfig—— Obtain link-local address using autoconfiguration.

dhcp—— Obtain a ipv6 address using dhcp.

enable—— Enable IPv6 on interface.

gateway—— Config IPv6 gateway.

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

The IPv6 interface subcommands:

```
Device (config-if)# ipv6 address fe80::192.168.0.1 eui-64
```

4.4 shutdown

Description

The **shutdown** command is used to shutdown the specified interface.

Syntax

shutdown

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Shutdown the specified interface:

```
Device (config-if)# shutdown
```

4.5 clear

Description

The **clear** command is used to reset functions.

Syntax

clear { access-list *acl-id* [*rule*] | arp-chche | counters [interface [fastEthernet *list* | gigabitEthernet *list* | port-channel *list* | ten-gigabitEthernet *list*]] | ethernet-oam {event-log [interface [fastEthernet *list* | gigabitEthernet *list*]] | statistics [interface [fastEthernet *list* | gigabitEthernet *list*]]} | ip {dhcp server {binding [*ipaddr*] | statistics} | igmp snooping statistics} | ipv6 {mld snooping statistics | nd detection statistics} | line *tid* | lldp statistics | logging [buffer | flash] | mac address-table {dynamic | filtering | static} | service-port *id*}

Parameter

acl-id——Specify the ACL ID or name.

rule—— Specify the ACL rule ID.

fastEthernet—— FastEthernet interface number list.

gigabitEthernet—— GigabitEthernet interface number list.

port-channel—— Port-channel interface number.

ten-gigabitEthernet—— Ten-gigabitEthernet interface number list.

Binding—— Clear all DHCP Server bindings.

statistics—— Clear DHCP Server statistics.

idaddr—— IP address.

snooping—— Clear all statistics for IGMP Snooping.

tid—— The ID of the reset terminal line.

statistics—— Clear LLDP statistics.

buffer—— Clear log in buffer.

flash—— Clear log in flash.

dynamic—— Clear all the dynamic address.

filtering—— Clear all the filtering MAC address.

static—— Clear all the static MAC address.

id—— Service virtual port ID.

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Reset functions:

```
Device (config-if)# clear access-list 1 rule 1
```

4.6 end

Description

The **end** command is used to return to Privileged EXEC Mode.

Syntax

end

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Return to Privileged EXEC Mode:

```
Device (config-if)# end
```

4.7 exit

Description

The **exit** command is used to exit current mode.

Syntax

exit

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Exit current mode:

```
Device (config-if)# exit
```

4.8 history

Description

The **history** command is used to display command history.

Syntax

history

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display command history:

```
Device (config-if)# history
```

4.9 no

Description

The **no** command is used to negate system information.

Syntax

no{description | ip {address *address mask* [gateway *gateway*] | dhcp option12} | ipv6 {address {*address* [eui-64] | *global-address* [eui-64] | dhcp} | enable | gateway *gateway*} | shutdown}

Parameter

address—— Specify the static IP address.

mask—— Specify the IP subnet mask.

gateway—— Specify the gateway.

global-address—— Config global IPv6 address manully.

enable—— Enable IPv6 on interface.

Shutdown—— shutdown the specified interface.

Command Mode

Interface Configuration Mode (interface Management)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Negate system information:

```
Device (config-if)# no ip address 192.168.0.1 255.255.255.0 gateway
10.0.0.1
```

Chapter 5 System Configuration Commands

System Commands can be used to configure the System information and System IP, reboot and reset the Device, upgrade the Device system and other operations.

5.1 system-time manual

Description

The **system-time manual** command is used to configure the system time manually.

Syntax

system-time manual *time*

Parameter

time —— Set the date and time manually, MM/DD/YYYY-HH:MM:SS. The valid value of the year ranges from 2000 to 2037.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system mode as manual, and the time is 12/20/2010 17:30:35

Device (config)# system-time manual 12/20/2010-17:30:35

5.2 system-time ntp

Description

The **system-time ntp** command is used to configure the time zone and the IP address for the NTP Server. The Device will get UTC automatically if it has connected to an NTP Server.

Syntax

system-time ntp { *timezone* } { *ntp-server* } { *backup-ntp-server* } { *fetching-rate* }

Parameter

timezone —— Your local time-zone, and it ranges from UTC-12:00 to UTC+13:00.

The detailed information that each time-zone means are displayed as follow:

UTC-12:00 —— TimeZone for International Date Line West.

UTC-11:00 —— TimeZone for Coordinated Universal Time-11.

UTC-10:00 —— TimeZone for Hawaii.

UTC-09:00 —— TimeZone for Alaska.

UTC-08:00 —— TimeZone for Pacific Time (US Canada).

UTC-07:00 —— TimeZone for Mountain Time (US Canada).

UTC-06:00 —— TimeZone for Central Time (US Canada).

UTC-05:00 —— TimeZone for Eastern Time (US Canada).

UTC-04:30 —— TimeZone for Caracas.

UTC-04:00 —— TimeZone for Atlantic Time(Canada).

UTC-03:30 —— TimeZone for Newfoundland.

UTC-03:00 —— TimeZone for Buenos Aires, Salvador, Brasilia.

UTC-02:00 —— TimeZone for Mid-Atlantic.

UTC-01:00 —— TimeZone for Azores, Cape Verde Is.

UTC —— TimeZone for Dublin, Edinburgh, Lisbon, London.

UTC+01:00 —— TimeZone for Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna.

UTC+02:00 —— TimeZone for Cairo, Athens, Bucharest, Amman, Beirut, Jerusalem.

UTC+03:00 —— TimeZone for Kuwait, Riyadh, Baghdad.

UTC+03:30 —— TimeZone for Tehran.

UTC+04:00 —— TimeZone for Moscow, St.Petersburg, Volgograd, Tbilisi, Port Louis.

UTC+04:30 —— TimeZone for Kabul.

UTC+05:00 —— TimeZone for Islamabad, Karachi, Tashkent.

UTC+05:30 —— TimeZone for Chennai, Kolkata, Mumbai, New Delhi.

UTC+05:45 —— TimeZone for Kathmandu.

UTC+06:00 —— TimeZone for Dhaka,Astana, Ekaterinburg.

UTC+06:30 —— TimeZone for Yangon (Rangoon).

UTC+07:00 —— TimeZone for Novosibrisk, Bangkok, Hanoi, Jakarta.

UTC+08:00 —— TimeZone for Beijing, Chongqing, Hong Kong, Urumqi, Singapore.

UTC+09:00 —— TimeZone for Seoul, Irkutsk, Osaka, Sapporo, Tokyo.

UTC+09:30 —— TimeZone for Darwin, Adelaide.

UTC+10:00 —— TimeZone for Canberra, Melbourne, Sydney, Brisbane.

UTC+11:00 —— TimeZone for Solomon Is., New Caledonia, Vladivostok.

UTC+12:00 —— TimeZone for Fiji, Magadan, Auckland, Welington.

UTC+13:00 —— TimeZone for Nuku'alofa, Samoa.

ntp-server —— The IP address for the Primary NTP Server.

backup-ntp-server —— The IP address for the Secondary NTP Server.

fetching-rate —— Specify the rate fetching time from NTP server.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system time mode as NTP, the time zone is UTC-12:00, the primary NTP server is 133.100.9.2 and the secondary NTP server is 139.78.100.163, the fetching-rate is 11 hours:

Device(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11

5.3 system-time dst predefined

Description

The **system-time dst predefined** command is used to select a daylight saving time configuration from the predefined mode. The configuration can be used recurrently. To disable DST function, please use **no system-time dst** command.

Syntax

system-time dst predefined [USA /Australia | Europe | New-Zealand]

no system-time dst

Parameter

USA /Australia | Europe | New-Zealand —— The mode of daylight saving time. There are 4 options which are USA, Australia, Europe and New-Zealand respectively. The default value is Europe.

Following are the time ranges of each option:

USA —— Second Sunday in March, 02:00 – First Sunday in November, 02:00.
Australia —— First Sunday in October, 02:00 – First Sunday in April, 03:00.
Europe —— Last Sunday in March, 01:00 – Last Sunday in October, 01:00.
New Zealand —— Last Sunday in September, 02:00 – First Sunday in April, 03:00.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the daylight saving time as USA standard:

Device(config)#system-time dst predefined USA

5.4 system-time dst date

Description

The **system-time dst date** command is used to configure the one-off daylight saving time. The start date is in the current year by default. The time range of the daylight saving time must shorter than one year, but you can configure it spanning years. To disable DST function, please use **no system-time dst** command.

Syntax

system-time dst date {*smonth*} {*sday*} {*stime*} {*syear*} {*emonth*} {*eday*} {*etime*} {*eyear*}[*offset*]

no system-time dst

Parameter

smonth——The start month of the daylight saving time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

sday—— The start day of the daylight saving time, ranging from 1 to 31. Here you should show special attention to February and the differences between a solar month and a lunar month.

stime—— The start moment of the daylight saving time, HH:MM.

syear—— The start year of the daylight saving time.

emonth—— The end month of the daylight saving time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

eday—— The end day of the daylight saving time, ranging from q to 31. Here you should show special attention to February and the differences between a solar month and a lunar month.

etime—— The end moment of the daylight saving time, HH:MM.

eyear—— The end year of the daylight saving time.

offset—— The number of minutes to add during the daylight saving time. It is 60 minutes by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the daylight saving time from zero clock, Apr 1st to zero clock Oct 1st and the offset is 30 minutes in 2015:

Device(config)# system-time dst date Apr 1 00:00 2015 Oct 1 00:00 2015 30

5.5 system-time dst recurring

Description

The **system-time dst recurring** command is used to configure the recurring daylight saving time. It can be configured spanning years. To disable DST function, please use **no system-time dst** command.

Syntax

system-time dst recurring {*sweek*} {*sday*} {*smonth*} {*stime*} {*eweek*} {*eday*} {*emonth*} {*etime*} [*offset*]

no system-time dst

Parameter

sweek——The start week of the daylight saving time. There are 5 values showing as follows: first, second, third, fourth, last.

sday—— The start day of the daylight saving time. There are 7 values showing as follows: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

smonth—— The start month of the daylight saving time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

stime—— The start moment of the daylight saving time, HH:MM.

eweek——The end week of the daylight saving time. There are 5 values showing as follows: first, second, third, fourth, last.

eday—— The end day of the daylight saving time. There are 5 values showing as follows: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

emonth—— The end month of the daylight saving time. There are 12 values showing as following: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

etime —— The end moment of the daylight saving time, HH:MM.

offset —— The number of minutes to add during the daylight saving time. It is 60 minutes by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the daylight saving time from 2:00am, the first Sunday of May to 2:00am, the last Sunday of Oct and the offset is 45 minutes:

Device(config)# system-time dst recurring first Sun May 02:00 last Sun Oct 02:00 45

5.6 hostname

Description

The **hostname** command is used to configure the system name. To clear the system name information, please use **no hostname** command.

Syntax

hostname [*hostname*]

no hostname

Parameter

hostname —— System Name. The length of the name ranges from 1 to 32 characters. By default, it is the device name, for example "T1600G-28TS".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system name as TPLINK:

Device(config)# hostname TPLINK

5.7 location

Description

The **location** command is used to configure the system location. To clear the system location information, please use **no location** command.

Syntax

location [*location*]

no location

Parameter

location —— Device Location. It consists of 32 characters at most. It is "SHENZHEN" by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system location as SHENZHEN:

Device(config)# location SHENZHEN

5.8 contact-info

Description

The **contact-info** command is used to configure the system contact information. To clear the system contact information, please use **no contact-info** command.

Syntax

contact-info [*contact_info*]

no contact-info

Parameter

contact_info —— Contact Information. It consists of 32 characters at most. It is "www.tp-link.com" by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the system contact information as www.tp-link.com:

```
Device(config)# contact-info www.tp-link.com
```

5.9 led

Note: This command is only available on certain devices.

Description

The **led** command is used to control the LEDs.

Syntax

led {on | off}

Parameter

on | off—— The LEDs are configured as on or off. By default, they are on.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the LED as off:

```
Device(config)# led off
```

5.10 ip address

Description

This **ip address** command is used to configure the IP address and IP subnet mask for the specified interface manually. The interface type includes: routed port, port-channel interface, loopback interface and VLAN interface.

Syntax

ip address { *ip-addr* } { *mask* } [secondary]

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

Parameter

ip-addr —— The IP address of the Layer 3 interface.

mask —— The subnet mask of the Layer 3 interface.

secondary —— Specify the interface's secondary IP address. If this parameter is omitted here, the configured IP address is the interface's primary address.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the VLAN interface 2 with the primary IP address as 192.168.1.1/24 and secondary IP address as 192.168.2.1/24:

Device (config)# interface vlan 2
Device (config-if)# ip address 192.168.1.1 255.255.255.0
Device (config-if)# ip address 192.168.2.1 255.255.255.0 **secondary**

5.11 ip address-alloc

Description

The **IP address-alloc** command is used to enable the DHCP Client function or the BOOTP Protocol. When this function is enabled, the specified interface will obtain IP from DHCP Server or BOOTP server. To disable the IP obtaining function on the specified interface, please use the **no ip address** command. This command applies to the routed port, the port-channel interface and the VLAN interface.

Syntax

ip address-alloc { dhcp | bootp }

no ip address

Parameter

dhcp —— Specify the Layer 3 interface to obtain IP address from the DHCP Server.

bootp —— Specify the Layer 3 interface to obtain IP address from the BOOTP Server.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Client function on the Lay 3 routed port 1/0/1:

Device (config)# interface gigabitEthernet 1/0/1

Device (config-if)# no switchport

Device (config-if)# ip address-alloc dhcp

Disable the IP address obtaining function on the VLAN interface 2:

Device (config)# interface vlan 2

Device (config-if)# no ip address

5.12 reset

Description

The **reset** command is used to reset the device's software. After resetting, all configuration of the device will restore to the factory defaults and your current settings will be lost.

Syntax

reset [except-ip]

Parameter

except-ip ——Maintain the IP address when resetting the device.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Reset all settings of the device except its IP address:

```
Device # reset except-ip
```

5.13 service reset-disable

Description

The **service reset-disable** command is used to disable the reset function of the console port or reset button. To enable the reset function, use **no service reset-disable** command. By default, the reset function is enabled.

Syntax

service reset-disable

no service reset-disable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Disable the reset function of console port or reset button:

```
Device (config)# service reset-disable
```

5.14 reboot

Description

The **reboot** command is used to reboot the device. To avoid damage, please don't turn off the device while rebooting.

Syntax

reboot

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Reboot the device:

```
Device # reboot
```

5.15 reboot-schedule

Description

This **reboot-schedule** command is used to configure the device to reboot at a certain time point. To delete the reboot schedule settings, please use the **reboot-schedule cancel** command.

Syntax

reboot-schedule at *time* [*date*] [save_before_reboot]

reboot-schedule in *interval* [save_before_reboot]

reboot-schedule cancel

Parameter

time —— Specify the time point for the device to reboot, in the format of hh:mm.

date —— Specify the date for the device to reboot, in the format of DD:MM:YYYY. The date should be within 30 days.

save_before_reboot —— Save the configuration file before the device reboots.

interval —— Specify a time period after which the device reboots. It ranges from 1 to 43200 minutes.

cancel —— Delete the reboot schedule settings.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

In the command **reboot-schedule at** *time* [*date*] [**save_before_reboot**], if no date is specified and the time you set here is later than the time that this command is executed, the device will reboot later that day; otherwise the device will reboot at the time point the next day.

Example

Specify the device to save the configuration files and reboot in 200 minutes:

Device (config)# reboot-schedule in 200 **save_before_reboot**

5.16 copy running-config startup-config

Description

The **copy running-config startup-config** command is used to save the current settings.

Syntax

copy running-config startup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Save current settings:

Device # copy running-config startup-config

5.17 copy startup-config tftp

Description

The **copy startup-config tftp** command is used to backup the configuration file to TFTP server.

Syntax

copy startup-config tftp ip-address *ip-addr* **filename** *name*

Parameter

ip-addr —— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name —— Specify the name for the configuration file which would be backup.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Backup the configuration files to TFTP server with the IP 192.168.0.148 and name this file config.cfg:

Device # copy startup-config tftp ip-address 192.168.0.148 **filename** config

Backup the configuration files to TFTP server with the IP fe80::1234 and name this file config.cfg:

Device # copy startup-config tftp ip-address fe80::1234 **filename** config

5.18 copy tftp startup-config

Description

The **copy tftp startup-config** command is used to download the configuration file to the device from TFTP server.

Syntax

copy tftp startup-config ip-address *ip-addr* **filename** *name*

Parameter

ip-addr —— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name —— Specify the name for the configuration file which would be downloaded.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Download the configuration file named as config.cfg to the device from TFTP server with the IP 192.168.0.148:

Device # copy tftp startup-config ip-address 192.168.0.148 **filename** config

Download the configuration file named as config.cfg to the device from TFTP server with the IP fe80::1234

Device # copy tftp startup-config ip-address fe80::1234 **filename** config

5.19 copy backup-config tftp

Description

The **copy backup-config tftp** command is used to export the backup configuration file of the device to TFTP server.

Syntax

copy backup-config tftp ip-address *ip-addr* **filename** *name*

Parameter

ip-addr —— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name —— Specify the name for the configuration file which would be exported.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Export the backup configuration file of the device to the TFTP server with the IP 192.168.0.148 and name the file config.cfg:

Device # copy backup-config tftp ip-address 192.168.0.148 **filename** config

5.20 copy backup-config startup-config

Description

The **copy backup-config startup-config** command is used to replace the startup configuration file using the backup configuration file.

Syntax

copy backup-config startup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Replace the startup configuration file using the backup configuration file.:

Device # copy backup-config startup-config

5.21 copy running-config backup-config

Description

The **copy running-config backup-config tftp** command is used to save the current running configuration as the backup configuration file.

Syntax

copy running-config backup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Save the current running configuration as the backup configuration file.

```
Device # copy running-config backup-config
```

5.22 copy tftp backup-config

Description

The **copy tftp backup-config** command is used to download the backup configuration file from a TFTP server.

Syntax

Copy tftp backup-config ip-address *ip-addr* **filename** *name*

Parameter

ip-addr —— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name —— Specify the name for the configuration file which would be downloaded.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Download the configuration file named config.cfg from the TFTP server with the IP 192.168.0.148:

Device # copy tftp backup-config ip-address 192.168.0.148 **filename** config

5.23 boot application

Description

The **boot application** command is used to configure the image file as startup image or backup image.

Syntax

boot application filename { image1 | image 2 } { startup | backup }

no boot application

Parameter

image1 | image2 —— Specify the image file to be configured. By default, the image1.bin is the startup image and the image2.bin is the backup image.

startup | backup —— Specify the property of the image, either startup image or backup image.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the image2.bin as the startup image:

Device (config)# boot application filename image2 startup

5.24 boot config

Description

The **boot config** command is used to configure the configuration file as startup configuration or backup configuration.

Syntax

boot config filename { config1 | config 2 } { startup | backup }

no boot application

Parameter

config1 | config2 —— Specify the configuration file to be configured. By default, the config1.cfg is the startup image and the config2.cfg is the backup image.

startup | backup—— Specify the property of the configuration.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the config2.cfg as the startup image:

```
Device (config)# boot config filename config2 startup
```

5.25 firmware upgrade

Description

The **firmware upgrade** command is used to upgrade the device's backup iamge file via the TFTP server. The uploaded firmware file will take place of the Backup Image, and user can choose whether to reboot the device with the Backup Image.

Syntax

firmware upgrade tftp ip-address *ip-addr* **filename** *name*

Parameter

ip-addr —— IP Address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

name —— Specify the name for the firmware file.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Upgrade the device's backup iamge file with the file firmware.bin in the TFTP server with the IP address 192.168.0.148, and reboot the device with this firmware:

Device # firmware upgrade tftp ip-address 192.168.0.148 **filename** firmware.bin

It will only upgrade the backup image. Continue? (Y/N):y

Operation OK!

Reboot with the backup image? (Y/N): y

Upgrade the device's backup iamge file with the file firmware.bin in the TFTP server with the IP address fe80::1234, but do not reboot the device:

Device # firmware upgrade tftp ip-address fe80::1234 **filename** firmware.bin

It will only upgrade the backup image. Continue? (Y/N):y

Operation OK!

Reboot with the backup image? (Y/N): n

5.26 ping

Description

The **ping** command is used to test the connectivity between the device and one node of the network.

Syntax

ping [ip | ipv6] { *ip_addr*} [-n *count*] [-l *size*] [-i *interval*]

Parameter

ip —— The type of the IP address for ping test should be IPv4.

ipv6 —— The type of the IP address for ping test should be IPv6.

ip_addr —— The IP address of the destination node for ping test. If the parameter ip/ipv6 is not selected, both IPv4 and IPv6 addresses are supported, for example 192.168.0.100 or fe80::1234.

-n *count* —— The amount of times to send test data during Ping testing. It ranges from 1 to 10. By default, this value is 4.

-l *size*—— The size of the sending data during ping testing. It ranges from 1 to 1500 bytes. By default, this value is 64.

-i *interval*—— The interval to send ICMP request packets. It ranges from 100 to 1000 milliseconds. By default, this value is 1000.

Command Mode

Privileged EXEC Mode

Privilege Requirement

None.

Example

To test the connectivity between the device and the network device with the IP 192.168.0.131, please specify the *count* (-l) as 512 bytes and *count* (-i) as 1000 milliseconds. If there is not any response after 8 times' Ping test, the connection between the device and the network device is failed to establish:

Device # ping 192.168.0.131 **–n** 8 **–l** 512

To test the connectivity between the device and the network device with the IP fe80::1234, please specify the *count* (-l) as 512 bytes and *count* (-i) as 1000 milliseconds. If there is not any response after 8 times' Ping test, the connection between the device and the network device is failed to establish:

Device # ping fe80::1234 **–n** 8 **–l** 512

5.27 tracert

Description

The **tracert** command is used to test the connectivity of the gateways during its journey from the source to destination of the test data.

Syntax

tracert [ip | ipv6] *ip_addr* [*maxHops*]

Parameter

ip —— The type of the IP address for tracert test should be IPv4.

ipv6 —— The type of the IP address for tracert test should be IPv6.

ip_addr —— The IP address of the destination device. If the parameter ip/ipv6 is not selected, both IPv4 and IPv6 addresses are supported, for example 192.168.0.100 or fe80::1234.

maxHops —— The maximum number of the route hops the test data can pass though. It ranges from 1 to 30. By default, this value is 4.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Test the connectivity between the device and the network device with the IP 192.168.0.131. If the destination device has not been found after 20 *maxHops*, the connection between the device and the destination device is failed to establish:

Device # tracert 192.168.0.131 20

Test the connectivity between the device and the network device with the IP fe80::1234. If the destination device has not been found after 20 *maxHops*, the connection between the device and the destination device is failed to establish:

Device # tracert fe80::1234 20

5.28 show system-info

Description

The **show system-info** command is used to display System Description, Device Name, Device Location, System Contact, Hardware Version, Firmware Version, System Time, Run Time and so on.

Syntax

show system-info

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the system information:

Device # show system-info

5.29 show image-info

Description

The **show image-info** command is used to display the information of image files in the system.

Syntax

show image-info

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system image files' information:

```
Device# show image-info
```

5.30 show boot

Description

The **show boot** command is used to display the boot configuration of the system.

Syntax

show boot

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system boot configuration information:

```
Device# show boot
```

5.31 show running-config

Description

The **show running-config** command is used to display the current operating configurations of the whole system, a specified unit, or a specified port.

Syntax

show running-config [*unit* {all | | [exclude *keyword*] [include *keyword*] | interface {fastEthernet |gigabitEthernet | ten-gigabitEthernet} *port*}]

show running-config [all | | [exclude *keyword*] [include *keyword*] | interface {fastEthernet |gigabitEthernet | ten-gigabitEthernet} *port*]

Parameter

unit—— Specify the unit number of a device to show the unit's operating configurations. By default, it is 1.

all—— Display all the operating configurations of the whole system or a specified unit.

|—— Enable filter to filtrate the configurations. You can use exclude and include to set the filter rule.

keyword—— The filter conditions, such as interface, vlan, and user.

port—— Specify the number of the port to show the port's operating configurations.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the current operating configurations only related to the user:

Device# show running-config | include user

5.32 show startup-config

Description

The **show startup-config** command is used to display the current configuration saved in the device. These configuration settings will not be lost the next time you reboot the device.

Syntax

show startup-config

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the saved configuration:

```
Device# show startup-config
```

5.33 show system-time

Description

The **show system-time** command is used to display the time information of the device.

Syntax

show system-time

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the time information of the device

```
Device# show system-time
```

5.34 show system-time dst

Description

The **show system-time dst** command is used to display the DST information of the device.

Syntax

show system-time dst

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DST information of the device

```
Device# show system-time dst
```

5.35 show system-time ntp

Description

The **show system-time ntp** command is used to display the NTP mode configuration information.

Syntax

show system-time ntp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the NTP mode configuration information of the device:

```
Device# show system-time ntp
```

5.36 show cpu-utilization

Description

The **show cpu-utilization** command is used to display the system's CPU utilization in the last 5 seconds/1minute/5minutes.

Syntax

show cpu-utilization

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the CPU utilization information of the device:

```
Device# show cpu-utilization
```

5.37 show memory-utilization

Description

The **show memory-utilization** command is used to display the current memory usage.

Syntax

show memory-utilization

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the memory utilization information of the device:

```
Device# show memory-utilization
```

5.38 dpms remote-address

Description

The **The dpms remote-address** command is used to select the interface you created in L3 Features and configure it as the interface to communicate with DPMS. This command is commonly used for the device to be managed by the DPMS in the same LAN or VLAN.

Syntax

dpms remote-address {address *ip-address*} [port *port-num*]

no dpms remote-address

Parameter

ip-address—— The IP address of the DPMS server.

port-num—— The listening port specified by the DPMS server, if not filled in, the default is 19810.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

The OLT advertises the existence of the machine to the DPMS through the discovery message:

```
Device(config)# dpms remote-address address 192.168.0.1 port 19810
```

5.39 dpms interface-id

Description

The **dpms interface-id** command is used to enter the remote IP address of your DPMS to tell the device where to discover the DPMS. This command is commonly used for the device to be managed by the DPMS in Layer 3 deployments.

Syntax

dpms interface-id *id*

Parameter

id—— Sets the current L3 interface to the specified port number through which the OLT sends Discovery message. This L3 interface is used by DPMS.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

The OLT advertises the existence of the machine to the DPMS through the discovery message:

```
Device(config-if)# dpms interface-id 2
```

5.40 show dpms remote-address

Description

The **show dpms remote-address** command is used to display the configured remote DPMS information, including IP and port number.

Syntax

show dpms remote-address

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the configured remote DPMS information, including IP and port number:

```
Device(config)# show dpms remote-address
```

5.41 show dpms interface

Description

The **show dpms interface** command is used to display the OLT Layer 3 interface where the configured near-end DPMS is located.

Syntax

show dpms interface

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the OLT Layer 3 interface where the configured near-end DPMS is located:

```
Device(config)# show dpms interface
```

5.42 patch load

Description

The **patch load** command is used to load a patch file from a TFTP server into the patch area of the system. The patch is in the deactivated state and has not taken effect.

Syntax

patch load ip-address *ip-addr* **filename** *filename* **[vrf** *vrf-name***]**

Parameter

Ipaddr —— IP address of the TFTP server.

Filename —— Name of the patch file.

vrf-name —— VRF instance name (1-15 characters).

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Download the patch file named patch.bin from the TFTP server address with IP address 192.168.0.2 and specify the VRF instance named vrf1:

```
Device# patch load ip-address 192.168.0.146 filename patch.bin vrf vrf1
```

5.43 patch active

Description

The **patch active** command is used to temporarily run a deactivated patch loaded into the system patch area. When a deactivated patch is temporarily run, the patch is activated and takes effect. When the device is restarted, the patch that was activated before the restart will be deactivated. Users can perform the following three operations on the activated patch.

Syntax

patch avtive

Parameter

patch run —— Change the patch status to running.

patch deactive —— Change the patch status to deactivated.

patch delete —— Invalidate the patch and delete it from the patch area.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Activate all deactivated patches loaded into the system patch area:

```
Device# patch active
```

5.44 patch run

Description

The **patch run** command is used to permanently run an activated patch. When an activated patch is permanently run, the patch is in the running state. When the device is restarted, the patch that was in the running state before the restart will remain in the running state and take effect. Users can perform the following two operations on the running patch:

Syntax

patch run

Parameter

patch uninstall —— Return the patch from the running state to the activated state.

patch delete —— Invalidate the patch and delete it from the patch area.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Permanently run an activated patch:

```
Device# patch run
```

5.45 patch deactive

Description

The **patch deactive** command is used to deactivate an activated patch:

Syntax

patch deactive

Parameter

patch uninstall —— Return the patch from the running state to the activated state.

patch delete —— Invalidate the patch and delete it from the patch area.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Deactivate an activated patch:

```
Device# patch deactive
```

5.46 patch uninstall

Description

The **patch uninstall** command is used to uninstall a running patch and activate it:

Syntax

patch uninstall

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Uninstall a running patch and activate it:

```
Device# patch uninstall
```

5.47 patch delete

Description

The **patch delete** command is used to delete a patch in the deactivated, activated, or running state, invalidating the patch and deleting the patch file from the system patch area:

Syntax

patch delete

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Delete a patch:

```
Device# patch delete
```

5.48 show patch information

Description

The **show patch information** command is used to view the patch information of the current system:

Syntax

show patch information

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the patch information of the current system:

```
Device# show patch information
```

Chapter 6 Time Range Commands

With this feature, you can configure a time range and bind it to an ACL rule.

6.1 time-range

Description

The **time-range** command is used to create time-range entry for the device and enter Time-range Create Configuration Mode. After a time-range entry is created, you need to specify the date and time. A time-range can implement multiple time-ranges simultaneously as long as they do not conflict with each other. To delete the corresponding time-range configuration, please use **no time-range** command.

Syntax

time-range *name*

no time-range *name*

Command Mode

Global Configuration Mode

Parameter

name —— The time-range name, ranging from 1 to 16 characters.

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a time-range named "tRange1" for the device:

```
Device(config)# time-range tRange1
```

6.2 absolute

Description

The **absolute** command is used to create an absolute time-range for the time-range of the device. To delete the corresponding absolute time-range configuration, please use **no absolute** command.

Syntax

absolute from *start-date* **to** *end-date*

no absolute [*index*]

Parameter

start-date —— The start date in Absoluteness Mode, in the format of MM/DD/YYYY.

end-date —— The end date in Absoluteness Mode, in the format of MM/DD/YYYY.

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an absolute time-range for the device and specify the date extending from May 5th, 2017 through Oct. 5th, 2017:

Device(config)#time-range tRange1

Device(config-time-range)#absolute from 05/05/2017 **to** 10/05/2017

6.3 periodic

Description

The **periodic** command is used to create a periodic mode time-range for the time-range of the device. To delete the corresponding periodic mode time-range configuration, please use **no periodic** command.

Syntax

periodic start *start-time* **end** *end-time* **day-of-the-week** *week-day*

no periodic [*index*]

Parameter

start-time——Specify the start time in the format of HH:MM

end-time——Specify the end time in the format of HH:MM

week-day——In the format of 1-3, 6, daily, off-day, or working-day. For example, 1-3,6 represents Monday, Tuesday, Wednesday and Saturday; daily represents every day; off-day represents the weekends; working-day represents the working days.

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time-range tSeg1 with time from 8:30 to 12:00 at weekends:

Device(config)#time-range tSeg1

Device(config -time-range)#periodic start 08:30 **end** 12:00

day-of-the-week 6-7

6.4 holiday (time-range mode)

Description

The **holiday** command is used to create holiday mode time-range for the time-range of the device. When the holiday which is excluded from time-range occurs, the device will not supply power.

Syntax

holiday { exclude | include }

Parameter

exclude ——The time range will not take effect on holiday.

include —— The time range will take effect on holiday.

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a time-range entry named “tRange3” and configure time-range to exclude the holiday:

Device(config)#time-range tRange3

Device(config-time-range)#holiday exclude

6.5 holiday

Description

The **holiday** command is used to create holiday for the device. To delete the corresponding holiday configuration, please use **no holiday** command.

Syntax

holiday *name* **start-date** *start-date* **end-date** *end-date*

no holiday *name*

Parameter

name —— The holiday name, ranging from 1 to 16 characters.

start-date —— The start date of the holiday, in the format of MM/DD, for instance, 05/01.

end-date ——The end date of the holiday, in the format of MM/DD, for instance, 05/01.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a holiday named "holiday1" and configure the start date as October 1st and the end date as October 3rd:

```
Device(config)# holiday holiday1 start-date 10/01 end-date 10/03
```

6.6 show holiday

Description

The **show holiday** command is used to display the defined holiday.

Syntax

show holiday

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined holiday:

```
Device# show holiday
```

6.7 show time-range

Description

The **show time-range** command is used to display the defined time-range.

Syntax

show time-range [*time-range-name*]

Parameter

time-range-name —— Specify the time range name with 1 to 16 characters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined time-range:

```
Device# show time-range
```

Chapter 7 PON Port Configuration Commands

PON Port Configuration Commands can be used to configure the features for PON ports.

7.1 shutdown

Description

The **shutdown** command is used to disable a PON port. To enable this port again, please use **no shutdown** command.

Syntax

shutdown

no shutdown

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the PON port 1/0/3:

Device(config)# interface gpon 1/0/3

Device(config-if-gpon)# shutdown

Disable the PON ports 1/0/2-7:

Device(config)# interface range gpon 1/0/2-7

Device(config-if-range)# shutdown

7.2 downstream-fec

Description

The **downstream-fec** command is used to enable the FEC (Forward Error Correction) feature of a PON port. FEC enhances the reliability of downstream traffic by inserting reduntdant data into the packets. It is recommended that you enable FEC only when there is sufficient bandwidth. To disable FEC, please use **no downstream-fec** command.

Syntax

downstream-fec

no downstream-fec

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the FEC feature of PON port 1/0/3:

Device(config)# interface gpon 1/0/3

Device(config-if-gpon)# downstream-fec

7.3 key-exchange

Description

The **key-exchange** command is used to configure the interval between each time when the encryption keys are updated by the ONUs connected to the GPON port.

Syntax

key-exchange { *exchange_interval*| no_renew }

Parameter

exchange_interval—— The interval between each time when the encryption keys are updated by the ONUs connected to the GPON port. This value should be between 1 and 60 (min).

no_renew —— The encryption keys used by the ONUs are not updated.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)}

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the key-exchange interval of PON port 1/0/3 as 50:

```
Device(config)# interface gpon 1/0/3
Device(config-if-gpon)# key-exchange 50
```

7.4 dba-calculate-mode

Description

The **dba-calculate-mode** command is used to set the DBA (dynamic bandwidth allocation) mode of a GPON port. Users can configure different DBA modes to meet different delay and bandwidth requirements.

Syntax

dba-calculate-mode { min-delay | max-bw }

Parameter

min-delay —— Indicates the minimum bandwidth delay. In this mode, the bandwidth is issued in DBA calculation period which increases with the number of the transmission container (T-CONT). Therefore, the delay is short. This mode must be used for TDM (Time Division Multiplexing) services.

max-bw —— Indicates the maximum bandwidth delay. In this mode, the bandwidth is issued in DBA calculation period which is fixed to eight frames. Each frame is 125 us. This mode is used for services that are not sensitive to delay.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)}

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the dba-calculate-mode of PON port 1/0/3 as min-delay:

```
Device(config)# interface gpon 1/0/3
Device(config-if-gpon)# dba-calculate-mode min-delay
```

7.5 range

Description

The **range** command is used to set the maximum and minimum distance of the ONUs which are connected to the PON port. To disable the range configuration, please use **no range** command.

Syntax

range max-distance *max-distance* **min-distance** *min-distance*

Parameter

max-distance —— Set the maximum distance of the ONUs which are connected to the PON port. This value should be between 1 and 60 (km).

min-distance —— Set the minimum distance of the ONUs which are connected to the PON port. This value should be between 0 and 40 (km).

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)}

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the max-distance of PON port 1/0/3 as 50 and the min-distance as 20:

Device(config)# interface gpon 1/0/3

Device(config-if-gpon)# range max-distance 50 **min-distance** 20

7.6 long-laseront auto-detect

Description

The **long-laseront auto-detect** command is used to enable the auto-detection of rogue ONUs which are connected to the PON port. When there are rogue ONUs, the system can detect them and send a log. To disable this feature, please use **no long-laseront auto-detect** command.

Syntax

long-laseront auto-detect

no long-laseront auto-detect

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the long-laseront auto-detect feature of PON port 1/0/3:

Device(config)# interface gpon 1/0/3

Device(config-if-gpon)# long-laseront auto-detect

7.7 long-laseront auto-detect-interval

Description

The **long-laseront auto-detect-interval** command is used to configure the interval between each time when the GPON port auto-detects rogue ONUs.

Syntax

long-laseront auto-detect-interval *interval*

Parameter

interval—— The interval between each time when the GPON port auto-detects rogue ONUs. This value should be between 1 and 100 (min).

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)}

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the long-laseront auto-detect-interval of PON port 1/0/3 as 50:

Device(config)# interface gpon 1/0/3

Device(config-if-gpon)# long-laseront auto-detect-interval 50

7.8 long-laseront auto-isolate

Description

The **long-laseront auto-isolate** command is used to enable the auto-isolation of rogue ONUs which are connected to the PON port when the rogue ONUs are detected. To disable this feature, please use **no long-laseront auto-isolate** command.

Syntax

long-laseront auto-isolate

no long-laseront auto-isolate

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the long-laseront auto-isolate feature of PON port 1/0/3:

Device(config)# interface gpon 1/0/3

Device(config-if-gpon)# long-laseront auto-isolate

7.9 onu-isolate

Description

The **onu-isolate** command is used to enable or disable the communication function between ONUs under the port. When the **no onu-isolate** function under the port is enabled, the ONUs under the port will be able to communicate with each other. By default it is **onu-isolate** state.

Syntax

onu-isolate

no onu-isolate

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the onu-isolate feature of PON port 1/0/3:

```
Device(config)# interface gpon 1/0/3
Device(config)# onu-isolate
```

7.10 port-isolate

Description

The **port-isolate** command is used to enable or disable the function of isolating a PON port from other PON ports. When **port-isolate** is enabled, the PON port will not be able to communicate with other isolated PON ports. By default it is the **port-isolate** state.

Syntax

port-isolate

no port-isolate

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the port-isolate feature of PON port 1/0/3:

```
Device(config)# interface gpon 1/0/3
Device(config)# port-isolate
```

7.11 show interface gpon

Description

The **show interface gpon** command is used to display the information of the GPON port.

Syntax

show interface gpon *pon-id*

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the GPON port 1/0/3:

Device(config)# show interface gpon 1/0/3

Chapter 8 DBA Profile Configuration Commands

DBA (Dynamically Bandwidth Allocation) improves the efficiency of GPON upstream bandwidth by dynamically adjusting the bandwidth among the ONUs. DBA profiles are applied to T-CONTs, which are created in a line profile, to determine the desired bandwidth allocation for certain GPON lines.

When the default DBA profile cannot meet the service requirements, you can add DBA profiles according to the service requirements.

8.1 dba-profile

Description

The **dba-profile** command is used to create a DBA profile. To delete the DBA profile, please use **no dba-profile** command.

Syntax

dba-profile [profile-id *profile-id*] [profile-name *profile-name*] {type1 fix *fixed_bandwidth_value* | type2 assure *assure_bandwidth_value* | type3 assure *assure_bandwidth_value* max *max_bandwidth_value* | type4 max *max_bandwidth_value* | type5 fix *fixed_bandwidth_value* assure *assure_bandwidth_value* max *max_bandwidth_value*}

no dba-profile {[profile-id *profile-id*] | [profile-name *profile-name*]}

Parameter

profile-id—— The profile ID of the DBA profile. The profile ID is the unique identifier for the DBA profile. If you leave the profile ID as blank, the system autamatically assigns the profile ID.

profile-name—— The profile name of the DBA profile. If you leave the profile name as blank, the system autamatically assigns the profile name.

type1 fix *fixed_bandwidth_value*—— Indicates a DBA profile of the fixed bandwidth type. The fixed bandwidth is reserved for a specified ONU or certain services of the ONU. It cannot be used for other ONUs even when the upstream service stream is not transmitted on the ONU. This type of bandwidth is mainly used for services, such as TDM and VoIP, that have a high QoS requirement. (*fixed_bandwidth_value*: 128-1310720 (kbps))

type2 assure *assure_bandwidth_value*—— Indicates a DBA profile of the assured bandwidth type. The assured bandwidth is the available bandwidth of

an ONU when the ONU requires the bandwidth. When the actual service stream does not reach the assured bandwidth, the DBA mechanism of the device is used to allocate the remaining bandwidth to services of other ONUs. Because of the DBA mechanism that allocates the remaining bandwidth to services of other ONUs, the assured bandwidth has a poorer real-time performance than fixed bandwidth does. (*assure_bandwidth_value*: 128-1310720 (kbps))

type3 assure *assure_bandwidth_value* **max** *max_bandwidth_value* —— Indicates a DBA profile of the assured bandwidth + maximum bandwidth type. This type of bandwidth is the bandwidth of the combined type. When it is used, the user is allocated with a certain bandwidth and at the same time occupies certain bandwidths. The total bandwidth, however, cannot exceed the maximum bandwidth configured for the user. This type of bandwidth is mainly used for VoIP and IPTV service. (*assure_bandwidth_value*: 128-1310720 (kbps); *max_bandwidth_value*: 128-1310720 (kbps); *max_bandwidth_value >= assure_bandwidth_value*)

type4 max *max_bandwidth_value* —— Indicates a DBA profile of the maximum bandwidth type. This type of bandwidth is the maximum bandwidth that can be used by an ONU to meet the ONU bandwidth requirement to the greatest extent. It is used for services such as Internet access service. (*max_bandwidth_value*: 128-1310720 (kbps))

type5 fix *fixed_bandwidth_value* **assure** *assure_bandwidth_value* **max** *max_bandwidth_value* —— Indicates a DBA profile of the fixed bandwidth + assured bandwidth + maximum bandwidth type. This type of bandwidth is the bandwidth of the combined type. When it is used, the user is allocated with the fixed bandwidth that cannot be used by other users. In addition, the user can use the assured bandwidth when necessary and can occupy certain bandwidths. The total bandwidth, however, cannot exceed the maximum bandwidth configured for the user. (*fixed_bandwidth_value*: 128-1310720 (kbps); *assure_bandwidth_value*: 128-1310720 (kbps); *max_bandwidth_value*: 128-1310720 (kbps); *max_bandwidth_value >= fixed_bandwidth_value* + *assure_bandwidth_value*)

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a DBA profile named TP-Link with a type-1 fixed bandwidth of 1024kbit/s:

Device(config)# dba-profile profile-name TP-Link type1 fix 1024

8.2 show dba-profile

Description

The **show dba-profile** command is used to display the information of the DBA profile.

Syntax

show dba-profile { profile-id *profile-id* | profile-name *profile-name* | all [detail] }

Parameter

profile-id —— The profile ID of the DBA profile. The profile ID is the unique identifier for the DBA profile.

profile-name —— The profile name of the DBA profile.

all —— Display all the DBA profiles.

detail —— Display the configuration of all the DBA profiles in detail.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DBA profile of profile-id 1:

Device(config)# show dba-profile profile-id 1

Chapter 9 Line Profile Configuration Commands

A line profile is used to configure the DBA (Dynamic Bandwidth Allocation), T-CONT (Transmission Container), GEM (GPON encapsulation mode) ports, and GEM mapping rules about a GPON ONU line.

GEM (GPON Encapsulation Mode) ports are the basic transmission units in the GPON network. Different types of traffic from the ONU are mapped to different GEM ports according to the GEM Mapping rules. The T-CONT (Transmission Container) functions as a tunnel which contains several GEM ports. A DBA profile is applied to the T-CONT to control the bandwidth allocation among different T-CONTs.

When the ONU is registered, a line profile is applied to the ONU to control the GPON ONU line.

When the default line profile cannot meet the service requirements, you can add line profiles according to the service requirements.dba-profile.

9.1 ont-lineprofile gpon

Description

The **ont-lineprofile gpon** command is used to create a line profile. To disable the line profile, please use **no ont-lineprofile gpon** command.

Syntax

ont-lineprofile gpon {[profile-id *profile-id*] [profile-name *profile-name*]}

no ont-lineprofile gpon {[profile-id *profile-id*] | [profile-name *profile-name*]}

Parameter

profile-id—— The profile ID of the line profile. The profile ID is the unique identifier for the line profile. If you leave the profile ID as blank, the system automatically assigns the profile ID.

profile-name—— The profile name of the line profile. If you leave the profile name as blank, the system automatically assigns the profile name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a line profile named TP-Link:

Device(config)# ont-lineprofile gpon profile-name TP-Link

9.2 tcont

Description

The **tcont** command is used to add T-CONTs to a line profile. To disable the T-CONT, please use **no tcont** command.

Syntax

tcont *tcont-list* {dba-profile-id *profile-id* | dba-profile-name *profile-name* }

no tcont *tcont-id*

Parameter

tcont-list —— The list of T-CONT ID. This value should be between 1-127

profile-id —— The profile ID of the DBA profile which is bound to the T-CONTs.

profile-name —— The profile name of the DBA profile which is bound to the T-CONTs.

Command Mode

ONT Line Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add T-CONT 2 to the line profile 1, and the DBA profile 3 is bound to the T-CONT:

Device(config)# ont-lineprofile 1

Device(config-ont-lineprofile)# tcont 2 **dba-profile-id** 3

9.3 mapping mode

Description

The **mapping mode** command is used to set the GEM mapping mode of a line profile.

Syntax

mapping mode { vlan | priority | port | vlan-priority | port-vlan | port-vlan-priority | port-priority }

Parameter

vlan —— Indicates that user services are mapped to GEM ports based on VLANs.

priority —— Indicates that user services are mapped to GEM ports based on priorities.

vlan-priority —— Indicates that user services are mapped to GEM ports based on VLANs and priorities.

port —— Indicates that user services are mapped to GEM ports based on ONU ports.

port-vlan —— Indicates that user services are mapped to GEM ports based on ONU ports and VLANs.

port-priority —— Indicates that user services are mapped to GEM ports based on ONU ports and priorities.

port-vlan-prioriity —— Indicates that user services are mapped to GEM ports based on ONU ports, VLANs, and priorities.

Command Mode

ONT Line Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the GEM mapping mode of line profile 1 as vlan-priority:

Device(config)# ont-lineprofile gpon profile-id 1

Device(config-ont-lineprofile)# mapping mode vlan-priority

9.4 gem add

Description

The **gem add** command is used to add the GEM port to the T-CONT in the line profile. To delete the GEM port, please use **gem delete** command.

Syntax

gem add *gem-port-id* **tcont** *tcont-id* [**encrypt** {enable | disable}]

gem delete *gem-port-id*

Parameter

gem-port-id——The GEM port ID. This value should be between 1 and1023.

tcont-id—— The T-CONT ID which the GEM port is bound to.

encrypt {enable | disable} —— Enable or disable the encryption feature of the GEM port.

Command Mode

ONT Line Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add GEM Port 3 to the T-CONT 2 in line profile 1 and enable the encryption feature of the GEM port

Device(config)# ont-lineprofile gpon profile-id 1

Device(config-ont-lineprofile)# gem add 3 tcont 2 encrypt enable

9.5 gem mapping

Description

The **gem mapping** command is used to add the GEM mapping rule in the line profile. The user service traffic is mapped to the GEM port based on the GEM mapping rule. To delete the GEM mapping rule, please use **no gem mapping** command.

Syntax

- If the mapping mode is vlan:

gem mapping *gem-port-id mapping-id* **vlan-transparent**

- If the mapping mode is vlan / priority / vlan-priority:

gem mapping *gem-port-id mapping-id* {vlan *vlan-id*| priority *priority*}

gem mapping *gem-port-id mapping-id* **vlan-untag**

- If the mapping mode is port / port-vlan / port-priority / port-vlan-priority:

gem mapping *gem-port-id mapping-id* **eth** *ont-port-id* [vlan *vlan-id* | priority *priority*]

gem mapping *gem-port-id mapping-id* **pots**[vlan *vlan-id*] [priority *priority*]

no gem mapping *gem-port-id mapping-id*

Parameter

gem-port-id——The GEM port ID.

mapping-id—— The GEM mapping ID. This value shoud be between 1 and 8.

vlan-id—— The VLAN ID which is mapped to the GEM port.

vlan

priority—— The priority which is mapped to the GEM port.

vlan-untag—— Indicates that untagged traffic is mapped to the GEM port

eth *ont-port-id*—— Indicates that the traffic from the ETH port is mapped to the GEM port.

pots—— Indicates that the traffic from POTS port is mapped to the GEM port.

vlan-transparent—— When configuring the mapping relationship as VLAN mapping using the "mapping-mode" command, this parameter is used to map all service flows to specific GEM Index. This mapping is globally unique, and no other types of GEM mapping mappings are allowed when this mapping exists.

Command Mode

ONT Line Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add GEM mapping rule 3 to the line profile 1, and service traffic in VLAN 2 with priority 3 is mapped to GEM port 2 based on this GEM mapping rule.

```
Device(config)# ont-lineprofile gpon profile-id 1
Device(config-ont-lineprofile)# gem mapping 2 3 vlan 2 priority 3
```

9.6 fec-upstream

Description

The **fec-upstream** command is used to enable the FEC (Forward Error Correction) feature of the ONT line profile. FEC enhances the reliability of

upstream traffic by inserting reduntdant data into the packets. It is recommended that you enable FEC only when there is sufficient bandwidth. To disable FEC, please use **no fec-upstream** command.

Syntax

fec-upstream

no fec-upstream

Command Mode

ONT Line Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the fec-upstream feature of the line profile 1

```
Device(config)# ont-lineprofile gpon profile-id 1
Device(config-ont-lineprofile)# fec-upstream
```

9.7 omcc encrypt

Description

The **omcc encrypt** command is used to enable the OMCC (ONT Management and Control Channel) encryption feature of the ONT line profile. When OMCC encryption is enabled, the OMCI traffic is encrypted. To disable this feature, please use **no omcc encrypt** command. By default, OMCC encryption is disabled.

Syntax

omcc encrypt

no omcc encrypt

Command Mode

ONT Line Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the OMCC encryption feature of the line profile 1

```
Device(config)# ont-lineprofile gpon profile-id 1
Device(config-ont-lineprofile)# omcc encrypt
```

9.8 show ont-lineprofile gpon

Description

The **show ont-lineprofile gpon** command is used to display the information of the GPON ONT line profile.

Syntax

show ont-lineprofile gpon {all | profile-id *profile-id* | profile-name *profile-name*}

Parameter

all —— Display all the line profiles.

profile-id —— The profile ID of the line profile. The profile ID is the unique identifier for the line profile.

profile-name —— The profile name of the line profile.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the line profile of profile-id 1:

```
Device(config)# show ont-lineprofile gpon profile-id 1
```

9.9 show ont-lineprofile gpon bound-info

Description

The **show ont-lineprofile gpon bound-info** command is used to display the ONUs which the line profile is bound to.

Syntax

show ont-lineprofile gpon bound-info {profile-id *profile-id* | profile-name *profile-name*}

Parameter

profile-id —— The profile ID of the line profile.

profile-name —— The profile name of the line profile.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bound-info of line profile 1:

```
Device(config)# show ont-lineprofile gpon bound-info profile-id 1
```

Chapter 10 Service Profile Configuration Commands

Service profiles determines parameter settings for services on an ONU managed by an OLT via OMCI (ONU Management Control Interface), including ONU port numbers of different types, multicast settings, port settings for transmitting user services, and so on.

When the default service profile cannot meet the service requirements, you can add service profiles according to the service requirements.

10.1 ont-srvprofile gpon

Description

The **ont-srvprofile gpon** command is used to create a service profile. To disable the service profile, please use **no ont-srvprofile gpon** command.

Syntax

ont-srvprofile gpon {[profile-id *profile-id*] [profile-name *profile-name*]}

no ont-srvprofile gpon {[profile-id *profile-id*] | [profile-name *profile-name*]}

Parameter

profile-id—— The profile ID of the service profile. The profile ID is the unique identifier for the service profile. If you leave the profile ID as blank, the system autamatically assigns the profile ID.

profile-name—— The profile name of the service profile. If you leave the profile name as blank, the system autamatically assigns the profile name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a service profile named TP-Link:

```
Device(config)# ont-srvprofile gpon profile-name TP-Link
```

10.2 ont-port

Description

The **ont-port** command is used to configure how many ports of different types are supported by the ONT bound with this service profile. By default, the port number of each type is 0.

Syntax

ont-port eth {*eth-port-num* | adaptive *max-eth-number*}

ont-port pots {*pots-port-num* | adaptive *max-pots-number*}

Parameter

eth-port-num —— The number of ONT Ethernet ports. This value should be between 0 and 24.

adaptive *max-eth-number* —— The number of ONT Ethernet ports is adaptive to the actual ONU but should not exceed the maximum number. This value should be between 0 and 24.

pots-port-num —— The number of ONT POTS ports. This value should be between 0 and 4.

adaptive *max-pots-number* —— The number of ONT POTS ports is adaptive to the actual ONU but should not exceed the maximum number. This value should be between 0 and 4.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the eth-port-number of service profile 1 as adaptive, and the maximum number as 24:

```
Device(config)# ont-srvprofile gpon profile-id 1

Device(config-ont-srvprofile)# ont-port eth adaptive 24
```

10.3 mac-learning

Description

The **mac-learning** command is used to enable the MAC learing feature of the ONT. By default, MAC learning is enabled. To disable this feature, please use **no mac-learning** command.

Syntax

mac-learning

no mac-learning

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MAC learning feature of service profile 1:

Device(config)# ont-srvprofile gpon profile-id 1

Device(config-ont-srvprofile)# mac-learning

10.4 native-vlan

Description

The **native-vlan** command is used to configure whether the native VLAN is concerned by the ONU which is bound with this service profile. If the native-vlan is concern, the untagged packets from the user's side are tagged with the native VLAN. By default, the native-vlan is set as concern.

Syntax

native-vlan { concern | unconcern }

Parameter

concern —— The native VLAN is concerned by the ONU.

unconcern —— The native VLAN is not concerned by the ONU.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the native-vlan as concern in service profile 1:

```
Device(config)# ont-srvprofile gpon profile-id 1
Device(config-ont-srvprofile)# native-vlan concern
```

10.5 multicast-mode

Description

The **multicast-mode** command is used to configure the mode of multicast traffic in the service profile. By default, the multicast-mode is set as unconcern.

Syntax

multicast-mode { unconcern | igmp-snooping | olt-control }

Parameter

unconcern —— The multicast mode is not determined by the service profile, but by the settings of the ONU.

igmp-snoopoing —— The ONU is required to maintain multicast forwarding tables.

olt-control —— The OLT is required to maintain multicast forwarding tables.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the multicast-mode as igmp-snooping in service profile 1:

```
Device(config)# ont-srvprofile gpon profile-id 1
Device(config-ont-srvprofile)# multicast-mode igmp-snooping
```

10.6 multicast-forward

Description

The **multicast-forward** command is used to configure the mode of multicast forwading in the service profile. By default, the multicast-forward is set as unconcern.

Syntax

multicast-forward {unconcern | untagged | tagged {transparent | translation *vlan-id*}}

Parameter

unconcern —— The mode of multicast forwarding is not determined by the service profile, but by the settings of the ONU.

untagged—— The downlink traffic forwarded by the ONU is untagged. Select the untagged mode if the ONU is directly connected to the STB (set-top box) or PC.

tagged—— The downlink traffic forwarded by the ONU is tagged. Select the tagged mode if the ONU is directly connected to the home gateway. If multicast-forward is set as tagged, you need to set the VLAN parameters.

transparent—— The multicast VLAN on the ISP's side is the same as that on the user's side.

translation *vlan-id* —— The multicast VLAN on the ISP's side is translated to the specified vlan-id on the user's side. The value of vlan-id should be between 1 and 4094.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the multicast-forward as untagged in service profile 1:

Device(config)# ont-srvprofile gpon profile-id 1

Device(config-ont-srvprofile)# multicast-forward untagged

10.7 priority-policy

Description

The **priority-policy** command is used to configure the priority of the uplink traffic of the ONU which is bound with the service profile. By default, the priority-policy is unconcern.

Syntax

port priority-policy eth *ont-port-id* { unconcern | assigned | copy-cos }

Parameter

ont-port-id —— The ONU port where the priority-policy is set.

unconcern —— The priority-policy is not determined by the service profile, but by the settings of the ONU.

assigned——The priority is assigned by the OLT.

copy-cos—— The priority of the uplink traffic is the same as the COS priority of the packets from the user.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the priority-policy of port 2 as copy-cos in service profile 1:

```
Device(config)# ont-srvprofile gpon profile-id 1
Device(config-ont-srvprofile)# port priority-policy eth 2 copy-cos
```

Example

Set the priority-policy of port 2 as copy-cos in service profile 1:

```
Device(config)# ont-srvprofile gpon profile-id 1
Device(config-ont-srvprofile)# port priority-policy eth 2 copy-cos
```

10.8 port igmp-forward

Description

The **port igmp-forward** command is used to configure the mode of IGMP forwading in the service profile. By default, the igmp-forward is set as unconcern.

Syntax

port igmp-forward eth *ont-port-list* {{{translation | default} *vlan-id* [*priority*]} | transparent | unconcern}

Parameter

ont-port-id—— The ONU port where the igmp-forward is set.

unconcern —— The mode of IGMP forwarding is not determined by the service profile, but by the settings of the ONU.

translation *vlan-id* [priority] —— The IGMP VLAN and priority on the user's side is translated to the specified vlan-id and priority on the ISP's side. The value of vlan-id should be between 1 and 4094. The priority should be between 0 and 7, and this parameter is optional.

default *vlan-id* [priority] —— The packets from the user's side are added with a outer layer of VLAN tag and then forwarded to the ISP's side. The value of vlan-id should be between 1 and 4094. The priority should be between 0 and 7, and this parameter is optional.

transparent—— The IGMP VLAN and priority on the ISP's side is the same as that on the user's side.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the igmp-forward of port 2 as transparent in service profile 1:

```
Device(config)# ont-srvprofile gpon profile-id 1

Device(config-ont-srvprofile)# port igmp-forward eth 2 transparent
```

10.9 port q-in-q

Description

The **port q-in-q** command is used to configure the QinQ feature of the ONU port. By default, the q-in-q is set as unconcern.

Syntax

port q-in-q eth *ont-port-id* {unconcern | enable | disable}

Parameter

ont-port-id —— The ONU port where the q-in-q is set.

unconcern —— The settings of q-in-q is not determined by the service profile, but by the settings of the ONU.

enable —— The q-in-q is enabled by the ONU port.

disable —— The q-in-q is disabled by the ONU port.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the q-in-q of port 2 as enabled in service profile 1:

```
Device(config)# ont-srvprofile gpon profile-id 1

Device(config-ont-srvprofile)# port q-in-q eth 2 enable
```

10.10 max-mac-count

Description

The **max-mac-count** command is used to configure the maximum number of MAC learning entries of the ONU port. By default, the max-mac-count is set as unlimited.

Syntax

port eth *ont-port-id* **max-mac-count {** *mac-address-num* **|** unlimited **}**

Parameter

ont-port-id —— The ONU port where the max-mac-count is set. This value should be between 1 and 24

mac-address-num ——The maximum number of MAC learning entries of the ONU port. This value should be between 1 and 255

unlimited —— The number of MAC learning entries of the ONU port is unlimited.

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the max-mac-count of port 2 as 255 in service profile 1:

```
Device(config)# ont-srvprofile gpon profile-id 1
Device(config-ont-srvprofile)# port eth 2 max-mac-count 255
```

10.11 port vlan

Description

The **port vlan** command is used to configure the VLAN feature of the ONU port on the user's side. To disable the VLAN configuration of the ONU port, use **no port vlan** command.

Syntax

port vlan eth *ont-port-id-list* **transparent**

port vlan pots transparent

port vlan eth *ont-port-id-list* **trunk** *vlan-id* [*priority-val* | user-cos] [tls]

port vlan pots trunk *vlan-id* [*priority-val* | user-cos]

port vlan eth *ont-port-id-list* **translation** *vlan-id* [*priority-val* | user-cos] user-vlan *user-vlanid* [*cpriority-val*]

port vlan pots translation *vlan-id* [*priority-val* | user-cos] **user-vlan** *user-vlanid* [*cpriority-val*]

port vlan eth *ont-port-id-list* **q-in-q** *vlan-id* [*priority-val* | user-cos] **user-vlan** *user-vlanid* [*cpriority-val*]

port vlan pots q-in-q *vlan-id* [*priority-val* | user-cos] **user-vlan** *user-vlanid* [*cpriority-val*]

no port vlan eth *ont-port-id-list* {*vlan-id priority-val* | trunk *vlan-id* tls}

no port vlan pots *vlan-id* [*priority-val* | user-cos]

Command Mode

ONT Service Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

10.12 show ont-srvprofile gpon

Description

The **show ont-srvprofile gpon** command is used to display the information of the GPON ONT service profile.

Syntax

show ont-srvprofile gpon {all | profile-id *profile-id* | profile-name *profile-name*}

Parameter

all —— Display all the service profiles.

profile-id —— The profile ID of the service profile. The profile ID is the unique identifier for the service profile.

profile-name —— The profile name of the service profile.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the service profile of profile-id 1:

```
Device(config)# show ont-srvprofile gpon profile-id 1
```

10.13 show ont-srvprofile gpon bound-info

Description

The **show ont-srvprofile gpon bound-info** command is used to display the ONUs which the service profile is bound to.

Syntax

show ont-srvprofile gpon bound-info {profile-id *profile-id* | profile-name *profile-name*}

Parameter

profile-id —— The profile ID of the service profile.

profile-name —— The profile name of the service profile.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bound-info of service profile 1:

```
Device(config)# show ont-srvprofile gpon bound-info profile-id 1
```

Chapter 11 Traffic Profile Configuration Commands

In Traffic profile, you can set up desired rate limit for any traffic which uses this profile, such as the inbound and outbound traffic of service ports.

11.1 traffic-profile

Description

The **traffic-profile** command is used to create or modify a traffic profile. To delete the traffic profile, please use **no traffic-profile** command.

Syntax

traffic-profile {profile-name *profile-name* | profile-id *profileId* | cir *cir* | pir *pir* | cbs *cbs* | pbs *pbs* | priority {assigned | user-cos} | prival *prival* | inner-priority {none | assigned | user-cos} | inner-prival *innerPri* | priority-policy {local-setting | tag-in-package | tag-in-ingress-package } }

no traffic-profile { all | profile-id *profile-id* | profile-name *profile-name* }

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

11.2 show traffic-profile

Description

The **show traffic-profile** command is used to display the information of the traffic profile.

Syntax

show traffic-profile { profile-id *profile-id* | [profile-name *profile-name*] | all }

Parameter

profile-id—— The profile ID of the traffic profile. The profile ID is the unique identifier for the traffic profile.

profile-name—— The profile name of the traffic profile.

all—— Display all the traffic profiles.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the traffic profile of profile-id 1:

```
Device(config)# show traffic-profile profile-id 1
```

Chapter 12 Management Profile Configuration Commands

Management profiles are used to uniformly configure ONU management settings, including ONU WAN connection configuration, ONU Wireless configuration, ONU VoIP configuration, ONU CWMP configuration, ONU CATV configuration, etc. If you want to configure the above settings uniformly, you can create management profiles according to your needs.

12.1 ont-mgmtprofile

Description

The **ont-mgmtprofile** command is used to create or modify a management profile on the OLT. The **no ont-mgmtprofile** command is used to delete a management profile.

Syntax

ont-mgmtprofile gpon [profile-id *profile-id*| profile-name *profile-name*]*

no ont-mgmtprofile gpon {profile-id *profile-id*| profile-name *profile-name*}*

Parameter

profile-id——The profile ID of the management profile. The profile ID is the unique identifier for the management profile. If you leave the profile ID as blank, the system automatically assigns the profile ID. The value ranges from 1 to 127.

profile-name—— The profile name of the management profile. If you leave the profile name as blank, the system will automatically assign a name of "mgmt_profile_x", with "x" being the management profile ID. String type: It can consist of uppercase letters, lowercase letters, numbers, and underscores. The length can range from 1 to 32 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a management profile on the OLT:

Device(config)# ont-mgmtprofile gpon profile-name TP-Link

12.2 catv

Description

The **catv** command is used to configure CATV parameters. With this command, the fiber network administrator can set a series of parameters to support the transmission and reception of CATV signals over fiber, ensuring stable transmission of CATV signals and enabling end users to watch TV programs through related devices. The **no catv** command is used to delete the configured CATV configuration.

Syntax

catv {enable | disable}

no catv

Command Mode

ONT Management Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add CATV configuration:

Device(config-ont-mgmeprofile)# catv enble

12.3 sipuser

Description

The **sipuser** command is used to add a SIP (Session Initiation Protocol) user account. It enables the configuration of SIP user accounts to facilitate Voice over IP (VoIP) services. These user accounts allow for the initiation, modification, and termination of real-time voice and video communication sessions over the IP network. The **no sipuser** command is used to remove a specific SIP user account.

Syntax

sipuser {registration-server *reg-server* | sipusername *sipusername* | sippassword *sippassword* | registration-port *port* | proxy-server *server* | proxy-port *port* | outbound-server *server* | outbound-port *port*}*

no sipuser

Parameter

sipusername——The username of the SIP account. The length can range from 0 to 50 characters.

sippassword——The password of the SIP account. The length can range from 0 to 25 characters.

reg-server——The registration server address of the SIP account. The length can range from 1 to 40 characters.

server——The server of the SIP account. The length can range from 0 to 40 characters.

port——The port of the SIP server. The value ranges from 0 to 65535.

Command Mode

ONT Management Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add an SIP account in the management profile:

Device(config-ont-mgmtprofile)# sipuser sipusername TP-Link **sippassword** admin

12.4 wlan

Description

The **wlan** command is used to add WLAN (Wireless Local Area Network) configuration. It allows for the configuration of Wi-Fi networks, enabling wireless network connectivity. This command can be used to set parameters for the wireless network, such as the SSID (Service Set Identifier), encryption method, frequency band, etc., allowing terminal devices to connect to the network wirelessly. On the other hand, the **no wlan** command is used to

delete the configured WLAN configuration, clearing out any unwanted wireless network settings.

Syntax

wlan {2_4g 2_4g_ssid *ssid* [2_4g_hide_ssid {enable | disable} | 2_4g_security *security* | 2_4g_password *password* | 2_4g_mode *mode* | 2_4g_channel *channel* | 2_4g_channel_width *width* | 2_4g_radio {enable | disable}] * | 5g_ 5g_ssid *ssid* [5g_hide_ssid {enable | disable} | 5g_security *security* | 5g_password *password* | 5g_mode *mode* | 5g_channel *channel* | 5g_channel_width *width* | 5g_radio {enable | disable}]* }*

wlan band-steering ssid *ssid* [security *security* | ssid-password *password* | hide-ssid {enable | disable} | radio {enable | disable}]*

no wlan

Parameter

ssid——The SSID of the WLAN. The length can range from 1 to 32 characters.

security——The encryption method of the WLAN. The valid values are: no_security, wpa_psk_tkip_wpa2_psk_aes, wpa2_psk_aes, wpa2_psk_aes_wpa3_personal

password——The password of the WLAN. The length can range from 8 to 63 characters. When the security is set to no_security, this parameter is not applicable.

mode——The mode of the WLAN. The 2.4G valid values are: 802_11_n, 802_11_g_n, 802_11_b_g_n; the 5G valid values are: 802_11_ac, 802_11_ac_n, 802_11_a_n_ac.

channel——The frequency band of the WLAN. The 2.4G valid values are: auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13; the 5G valid values are: auto, 36, 40, 44, 48, 149, 153,157,161.

width——The frequency band width of the WLAN. The 2.4G valid values are: auto, 20, 40; the 5G valid values are: auto, 20, 40, 80.

Command Mode

ONT Management Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a WLAN configuration in the management profile:

Device(config-ont-mgmtprofile)# wlan 2_4g 2_4g_ssid TP-Link_1234

12.5 wan

Description

The **wan** command is used to create a new ONT WAN connection. It uniquely identifies a WAN connection using the wan-id parameter. If the WAN connection corresponding to the wan-id does not exist, a new one will be created. If it already exists, the WAN connection will be modified. The **no wan** command is used to delete a WAN connection.

Syntax

The WAN Connection type is Bridge:

wan *wan-id* **admin-status** {enable | disable} **conn-type bridge** {internet | internet-tr069 | internet-voip | internet-voip-tr069 | other | tr069 | voip | voip-tr069} *mtu-val* [vlan *vlan-id* priority *priority*] [lan-dhcp {enable | disable}] [conn-name *name*] [port-banding {eth *port_id_list* | wifi_2_4_g | wifi_5g_1 | wifi_5g_2}*]

The WAN Connection type is Dynamic-IP:

wan *wan-id* **admin-status** {enable | disable} **conn-type dynamic-ip** {internet | internet-tr069 | internet-voip | internet-voip-tr069 | other | tr069 | voip | voip-tr069} *mtu-val* [vlan *vlan-id* priority *priority*] [lan-dhcp {enable | disable}] [nat {enable | disable}] [conn-name *name*] {ipv4 dns-type {auto| manual {primary-dns *ipv4_addr* secondary-dns *ipv4_addr*}} [ipv4-default-gateway {enable | disable}] | ipv6 [dhcpv6 | slaac] dns-type {auto | manual {ipv6-primary-dns *ipv6_addr* ipv6-secondary-dns *ipv6_addr*}} [ipv6-default-gateway {enable | disable}]]* [port-banding {eth *port_id_list* | wifi_2_4_g | wifi_5g_1 | wifi_5g_2}*]

The WAN Connection type is PPPoE:

wan-pppoeprofile *wan-id*

pppoe-username *username*

pppoe-password *password*

wan *wan-id* **admin-status** {enable | disable} **conn-type pppoe** {internet | internet-tr069 | internet-voip | internet-voip-tr069 | other | tr069 | voip | voip-tr069} *mtu-val* [vlan *vlan-id* priority *priority*] [nat {enable | disable}]

[lan-dhcp {enable | disable}] [conn-name *name*] {ipv4 [ipv4-default-gateway {enable | disable}]| ipv6 {dhcpv6 | slaac} [ipv6-default-gateway {enable | disable}]} [port-banding {eth *port_id_list* | wifi_2_4_g | wifi_5g_1 | wifi_5g_2}*]

no wan *wan-id*

Parameter

wan-id——The ID of the WAN connection. The value ranges from 1 to 8.

bridge——The WAN connection type is bridge.

dynamic-ip——The WAN connection type is dynamic-ip.

pppoe——The WAN connection type is PPPoE.

internet——Indicates that the connection is used for the Internet.

internet-tr069——Indicates that the connection is used for Internet and TR069 services.

internet-voip——Indicates that the connection is used for Internet and voice services.

internet-voip-tr069——Indicates that the connection is used for Internet access, voice services and TR069 services.

other——Indicates that the connection is for IPTV service.

tr069——Indicates that the connection is used for TR069 service.

voip——Indicates that the connection is used for voice services.

voip-tr069——Indicates that the connection is used for voice and TR069 services.

mtu-val——Set MTU value.

vlan-id——Set the VLAN ID to which the WAN connection belongs. The value ranges from 1 to 4094.

priority——Set the priority of the WAN connection. The value ranges from 0 to 7.

lan-dhcp——Enable or disable the DHCP function of the LAN port.

nat——Enable or disable the NAT function of the WAN connection.

name——The name of the WAN connection. The length can range from 1 to 32 characters.

auto——Obtain DNS automatically.

manual——To manually set DNS, you need to set primary-DNS and secondary-DNS.

primary-dns——Set the IP of the manually configured primary DNS Server.

secondary-dns——Set the IP of the manually configured secondary DNS server.

username—— The username used by PPPOE for dialing.

password—— The password used by PPPOE dial.

IPv4_addr—— The static IP address for IPv4.

IPv6_addr—— The static IP address for IPv6.

ipv4-default-gateway——When the admin-status is enabled, set this connection as the default connection for IPv4.

ipv6-default-gateway——When the admin-status is enabled, set this connection as the default connection for IPv6.

dhcpv6——Set the IPV6 addressing type to DHCPv6.

slaac——Set the IPV6 addressing type to SLAAC.

port-id-list——The value range of the ONT port bound to the WAN connection. The valid values are: Port1-4, wifi_2_4_g, wifi_5g_1, wifi_5g_2.

Command Mode

ONT Management Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a new ONT WAN connection:

Device(config-ont-mgmtprofile)# wan 1 **admin-status enable conn-type bridge internet** 64 **vlan** 1 **priority** 0 **lan-dhcp enable conn-name** TP-Link **port-banding eth** 1

12.6 cwmp

Description

The **cwmp** command is specifically used to add the necessary configuration for enabling CPE WAN Management Protocol (CWMP). CWMP is a widely-used protocol that facilitates efficient remote management and configuration of customer premises equipment (CPE) in a wide area network (WAN) environment. The **no cwmp** command is used to delete the configured CWMP configuration.

Note: When connection authentication is enabled, you must first create a cwmp-auth-profile to input the required port, path, username, and password for the authentication.

Syntax

cwmp url *url* [username *acs-username* | pwd *acs-pwd* | cwmp-status {enable | disable} | inform-status{enable | disable} | inform-interval *inform-interval* | auth-status{enable | disable}]*

no cwmp

When the auth-status is enabled, create the cwmp-auth-profile first:

cwmp-auth-profile

conn-auth path *path* **port** *port*

auth-username *auth-username*

auth-password *auth-password*

Parameter

url——The address of the ACS URL. The length can range from 1 to 255 characters.

acs-username——The username of the ACS URL. The length can range from 0 to 50 characters.

acs-pwd——The password of the ACS URL. The length can range from 0 to 25 characters.

Inform-interval——The interval of inform messages. The value ranges from 1 to 4294967295.

path——The path of the authentication. The length can range from 1 to 15 characters and must start with a "/".

port——The port of the authentication. The interval of inform messages. The value ranges from 1000 to 65535.

auth-username——The username of the authentication. The length can range from 0 to 255 characters.

auth-password——The password of the authentication. The length can range from 0 to 255 characters.

Command Mode

ONT Management Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a CWMP configuration on a management profile:

```
Device(config-ont-mgmtprofile)# cwmp-auth-profile
Device(config-mgmtprofile-cwmp-auth)# conn-auth path /192.168.1.1
port 1000
```

12.7 show ont-mgmtprofile gpon

Description

The **show ont-mgmtprofile gpon** command is used to display management profile information.

Syntax

show ont-mgmtprofile gpon {all | profile-id *profile-id* | profile-name *profile-name*}

Parameter

all—— Display all management profile information.

profile-id——The ID of the management profile. The value ranges from 1 to 127.

profile-name——The name of the management profile. It can consist of uppercase and lowercase letters, numbers, and underscores, with a length ranging from 1 to 32 characters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display all management profile information:

```
Device# show ont-mgmtprofile gpon all
```

12.8 show ont-mgmtprofile gpon bound-info

Description

The **show ont-mgmtprofile gpon bound-info** command is used to query the binding information of a specified GPON ONT management profile.

Syntax

show ont-mgmtprofile gpon bound-info {profile-id *profile-id*| profile-name *profile-name*}

Parameter

profile-id——The ID of the management profile. The value ranges from 1 to 127.

profile-name——The name of the management profile. It can consist of uppercase and lowercase letters, numbers, and underscores, with a length ranging from 1 to 32 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Query the binding information of the management profile 1:

```
Device# show ont-mgmtprofile gpon bound-info profile-id 1
```

12.9 remote-access

Description

The **remote-access** command is used to create/modify the remote-access configuration in the ONT management profile. The **no remote-access** command is used to clear the configuration.

Syntax

remote-access {enable|disable}

no remote-access

Command Mode

ONT Management Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the remote-access configuration in the ONT management profile:

```
Device(config-ont-mgmtprofile)# remote-access enable
```

Chapter 13 ONU-Register Commands

After connecting the ONU to the GPON network, the ONU is auto-found by the OLT. Then you need to authenticate and register the ONU. You can also set auto authentication for ONUs. After the ONU is registered, the ONU goes online and is able to communicate with the OLT via the GPON network.

13.1 ont autofind

Description

The **ont autofind** command is used to enable the autofind feature of the ONT. To disable autofind, please use **no ont autofind** command.

Syntax

ont autofind

no ont autofind

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

13.2 ont autofind timeout

Description

The **ont autofind timeout** command is used to set the aging time of the auto-found ONT.

Syntax

ont autofind {timeout *time* | no-aging}

Parameter

time —— The aging time of the auto-found ONT.

no-aging—— No setting the aging time of the auto-found ONT.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the aging time of the auto-found ONT to 100s:

```
Device(config)# ont autofind timeout 100
```

13.3 ont autofind interval

Description

The **ont autofind interval** command is used to set the interval between each time the OLT auto-find the ONTs.

Syntax

ont autofind interval *time*

Parameter

time —— The interval between each time the OLT auto-find the ONTs.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the interval between each time the OLT auto-find the ONTs to 1s:

```
Device(config-if-gpon)# ont autofind interval 1
```

13.4 ont cancel

Description

The **ont cancel** command is used to clear the information of auto-found ONTs.

Syntax

ont cancel {all | *sn-val*}

Parameter

all—— All of the ONTs

sn-val—— The SN value in the auto-found ONTs list.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear all the information of auto-found ONTs.:

```
Device(config-if-gpon)# ont cancel all
```

13.5 ont confirm

Description

The **ont confirm** command is used to confirm and register autofound ONT.

Syntax

(1) Authenticate the ONT using password:

ont confirm password-auth password-type {asci | hex }*password-val* { always-on | once-on} [{sn | sn-password}] {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont *ont-id*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(2) Authenticate the ONT using SN:

ont confirm sn-auth *sn-val* {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont *ont-id*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(3) Authenticate the ONT using LOID:

ont confirm loid-auth *loid-val* { always-on | once-on} {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont *ont-id*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(4) Authenticate the ONT using password and LOID:

ont confirm loid-and-password-auth *loid-val loid-password*{ always-on | once-on} {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*] } {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont *ont-id*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(5) Authenticate the ONT using password and SN:

ont confirm sn-and-password-auth *sn-val password-val* {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont *ont-id*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

Parameter

ont-id—— The ONT-ID assigned to the ONT, if not specified, the system automatically assigns the smallest ont ID that is free under the current port.

sn-val—— The SN value of the autofound ONT.

password-type—— The password type of the autofound ONT.

password-val—— The password value of the autofound ONT.

loid-val—— The LOID value of the autofound ONT.

loid-password—— The LOID password value of the autofound ONT.

always-on—— According to different authentication methods, the first authentication will use password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will not be automatically matched, and each subsequent authentication will use the same authentication method as the first authentication. After the ONT is certified, it can go online even if the SN is modified.

once-on—— According to different authentication methods, the first authentication uses password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will be automatically matched, and each subsequent authentication will use the method of SN or SN+password/ SN+LOID / SN+LOID+password, which corresponds to the authentication method of the first authentication.

sn—— Configure the second and subsequent authentication to only verify the SN.

sn password—— Configure the second and subsequent authentication to verify the SN and password at the same time.

ont-lineprofile-id—— The line profile ID.

ont-lineprofile-name—— The line profile name.

ont-srvprofile-id—— The service profile ID.

ont-srvprofile-name—— The service profile name.

ont-mgmtprofile-id—— The management profile ID.

ont-mgmtprofile-name—— The management profile name.

desc——The description of the autofound ONT.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Authenticate with the password, confirm and register autofound ONTs:

Device(config-if-gpon)# ont confirm password-auth password-type asci admin always-on ont-lineprofile-id 0 ont-srvprofile-id 0

13.6 ont confirm all

Description

The **ont confirm** command is used to confirm and register autofound ONTs in batches.

Syntax

(1) Authenticate the ONT using password:

ont confirm all password-auth { always-on | once-on} [{sn | sn-password}]{[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id*| ont-mgmtprofile-name *profile-name*]*

(2) Authenticate the ONT using SN:

ont confirm all sn-auth {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*] } {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id*| ont-mgmtprofile-name *profile-name*]*

(3) Authenticate the ONT using LOID:

ont confirm all loid-auth { always-on | once-on} {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(4) Authenticate the ONT using password and LOID:

ont confirm all loid-and-password-auth { always-on | once-on} {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id*| ont-mgmtprofile-name *profile-name*]*

(5) Authenticate the ONT using password and SN:

ont confirm all sn-and-password-auth {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

Parameter

always-on—— According to different authentication methods, the first authentication will use password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will not be automatically matched, and each subsequent authentication will use the same authentication method as the first authentication. After the ONT is certified, it can go online even if the SN is modified.

once-on—— According to different authentication methods, the first authentication uses password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will be automatically matched, and each subsequent authentication will use the method of SN or SN+password/ SN+LOID / SN+LOID+password, which corresponds to the authentication method of the first authentication.

sn—— Configure the second and subsequent authentication to only verify the SN.

sn password—— Configure the second and subsequent authentication to verify the SN and password at the same time.

ont-lineprofile-id—— The line profile ID.

ont-lineprofile-name—— The line profile name.

ont-srvprofile-id—— The service profile ID.

ont-srvprofile-name—— The service profile name.

ont-mgmtprofile-id—— The management profile ID.

ont-mgmtprofile-name—— The management profile name.

desc——The description of the autofound ONT.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Authenticate with the password, confirm and register autofound ONTs in batches.:

Device(config-if-gpon)# ont confirm all password-auth always-on ont-lineprofile-id 0 ont-srvprofile-id 0

13.7 show ont autofind

Description

The **show ont autofind** command is used to display the information of autofound ONTs.

Syntax

show ont autofind { by-equipment-id *equip-id* | by-hardware-version *hardware-version* | by-loid *loid* | by-loid-password *loid-password* | by-password {asci | hex } *password* | by-sn *sn-val* | by-software-version *software-version* | by-vendor-id *vendor-id* | gpon *pon-port-list*}

Parameter

by-equipment-id——Display the information of autofound ONTs through equipment ID.

by-hardware-version——Display the information of autofound ONTs through hardware version.

by-software-version——Display the information of autofound ONTs through software version.

by-loid——Display the information of autofound ONTs through LOID.

by-loid-password——Display the information of autofound ONTs through LOID password.

by-password——Display the information of autofound ONTs through password.

by-sn——Display the information of autofound ONTs through SN.

by-vendor-id——Display the information of autofound ONTs through vendor id.

pon-port-list—— The PON port list.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of autofound ONTs configured by1/0/1:

```
Device(config)# show ont autofind 1/0/1
```

13.8 ont add

Description

The **ont add** command is used to add the method of ONT authentication and bind the profiles to the ONT. This command is maily used to add the ONT when the ONT is offline.

Syntax

(1) Authenticate the ONT using password:

ont add [*ont-id*] **password-auth password-type** {asci | hex } *password-val* { always-on | once-on {sn | sn-password}} {[ont-lineprofile-id *profile-id*] / [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*] } [desc *desc*] [ont-mgmtprofile-id *profile-id*| ont-mgmtprofile-name *profile-name*]*

(2) Authenticate the ONT using SN:

ont add [*ont-id*] **sn-auth** *sn-val* {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(3) Authenticate the ONT using LOID:

ont add [*ont-id*] **loid-auth** *loid-val* { always-on | once-on} {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] |

[ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(4) Authenticate the ONT using password and LOID:

ont add [*ont-id*] **loid-and-password-auth** *loid-val loid-password*{ always-on | once-on} {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]} [desc *desc*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

(5) Authenticate the ONT using password and SN:

ont add [*ont-id*] **sn-and-password-auth** *sn-val* **password-type** {asci | hex }*sn-val password-val* {[ont-lineprofile-id *profile-id*'] /[ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*] } [desc *desc*] [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

Parameter

ont-id—— The ONT-id assigned to the ONT, if not specified, the system automatically assigns the smallest ont id that is free under the current port.

password-auth—— Set the ONT authentication mode to password authentication.

password-val—— The password value of the ONT.

sn-auth—— Set the ONT authentication mode to SN authentication.

sn-val—— The SN value of the ONT.

loid-auth—— Set the ONT authentication mode to LOID authentication.

loid-val—— The LOID value of the ONT.

loid-password—— The LOID password value of setting ONT loid authentication.

loid-and-password-auth—— Set the ONT authentication mode to LOID and password authentication.

sn-and-password-auth—— Set the ONT authentication mode to SN and password authentication.

always-on—— According to different authentication methods, the first authentication will use password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will not be automatically matched, and each subsequent authentication will use the same authentication method as the first authentication. After the ONT is certified, it can go online even if the SN is modified.

once-on—— According to different authentication methods, the first authentication uses password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will be automatically matched, and each subsequent authentication will use the method of SN or SN+password/ SN+LOID / SN+LOID+password, which corresponds to the authentication method of the first authentication.

sn—— Configure the second and subsequent authentication to only verify the SN.

sn password—— Configure the second and subsequent authentication to verify the SN and password at the same time.

ont-lineprofile-id—— The line profile ID.

ont-lineprofile-name—— The line profile name.

ont-srvprofile-id—— The service profile ID.

ont-srvprofile-name—— The service profile name.

ont-mgmtprofile-id—— The management profile ID.

ont-mgmtprofile-name—— The management profile name.

desc——The description of the ONT.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Authenticate with the password "admin", add the method of ONT authentication and bind the profiles to the ONT:

```
Device(config-if-gpon)# ont add 0 password-auth password-type ascii
admin    always-on ont-lineprofile-id 0 ont srvprofile-id 0
```

13.9 ont activate

Description

The **ont activate** command is used to activate the ONT which is found by the OLT PON port. To deactivate the ONT, use **ont deactivate** command.

Syntax

ont activate *ontid-list*

ont deactivate *ontid-list*

Parameter

ontid-list—— The ont ID list of the ONT which is found by the OLT PON port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Activate the ONT 1-3 which is found by the OLT PON port:

```
Device(config-if-gpon)# ont activate 1-3
```

13.10 ont reset

Description

The **ont reset** command is used to reset the ONT which is found by the OLT PON port.

Syntax

ont reset *ontid-list*

Parameter

ontid-list—— The ont ID list of the ONT which is found by the OLT PON port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Reset the ONT 1-3 which is found by the OLT PON port:

```
Device(config-if-gpon)# ont reset 1-3
```

13.11 ont delete

Description

The **ont delete** command is used to delete the ONT which is found by the OLT PON port. If the configuration of the ONT is incorrect, delete the ONT and then add it again.

Syntax

ont delete *ontid-list*

Parameter

ontid-list—— The ont ID list of the ONT which is found by the OLT PON port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete the ONT 1-3 which is found by the OLT PON port:

```
Device(config-if-gpon)# ont delete 1-3
```

13.12 show ont auth-info

Description

The **show ont auth-info** command is used to display the authentication information of ONTs.

Syntax

show ont auth-info {by-active-status {active|inactive}| by-match-status {match|mismatch}| by-online-status {online|offline}| by-admin-status {activated|deactivated} | by-config-status {success|failed}| by-desc *desc* | by-line-profile {profile-id *id*| profile-name *name*}| by-srv-profile {profile-id *id*| profile-name *name*} | by-mgmt-profile {profile-id id | profile-name name} | by-loid *loid*| by-loid-password *loid-password*| by-sn *sn-val*| by-password password-type {asci | hex } *password*| gpon } *pon-port-list*

Parameter

by-active-status—— Display ONU authentication information through active status.

by-match-status—— Display ONU authentication information through match status.

by-online-status—— Display ONU authentication information through online status.

by-admin-status—— Display ONU authentication information through admin status.

by-config-status—— Display ONU authentication information through config status.

by-desc—— Display ONU authentication information through description.

by-line-profile—— Display ONU authentication information through line profile.

by-srv-profile—— Display ONU authentication information through srv profile.

by-mgmt-profile—— Display ONU authentication information through management profile.

by-loid—— Display ONU authentication information through LOID.

by-loid-password—— Display ONU authentication information through loid-password.

by-sn—— Display ONU authentication information through SN.

by-password—— Display ONU authentication information through password.

gpon—— Display ONU authentication information through the PON port.

pon-port-list—— The PON port list.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the authentication information of ONTs configured by 1/0/1:

```
Device(config)# show ont auth-info gpon 1/0/1
```

13.13 ont auto-auth

Description

The **ont auto-auth** command is used to enable the auto-authentication feature of the ONT. To disable this feature, please use **no ont auto-auth** command.

Syntax

ont auto-auth

no ont auto-auth

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

13.14 ont auto-auth match-mode

Description

The **ont auto-auth match-mode** command is used to configure the matching mode of the ONT in the auto-authentication process.

Syntax

Ont auto-auth match-mode { all-ont | equid-auth | equid-swver-auth | vendor-auth }

Parameter

all-ont—— All online ONTs support automatic authentication and registration; ONTs that have been configured with authentication policies are still authenticated and registered according to the authentication policies.

equid-auth—— Based on Equid matching, ONTs that meet the matching rules support automatic authentication and registration; ONTs that have been configured with an authentication policy still authenticate and register according to the authentication policy.

equid-swver-auth—— Based on Equid+Softwareversion matching, ONTs that meet the matching rules support automatic authentication and registration; ONTs that have been configured with authentication policies are still authenticated and registered according to the authentication policies.

vendor-auth—— Based on Vendor ID matching, ONTs that meet the matching rules support automatic authentication and registration; ONTs that have been configured with authentication policies still authenticate and register according to the authentication policies.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the matching method of ONTs during the auto-authentication process so that all online ONTs support auto-authentication and registration:

```
Device(config-if-gpon)# ont auto-auth match-mode all-ont
```

13.15 ont auto-auth authmode

Description

The **ont auto-auth authmode** command is used to configure the auto-authentication mode of the ONT.

Syntax

ont auto-auth authmode {loid-and-password-auth { always-on | once-on } | loid -auth { always-on | once-on } | password-auth { always-on | once-on {sn | sn-password}} | sn-auth |sn-and-password-auth}

Parameter

password-auth—— Set the ONT authentication mode to password authentication.

sn-auth—— Set the ONT authentication mode to SN authentication.

loid-auth—— Set the ONT authentication mode to LOID authentication.

sn-and-password-auth—— Set the ONT authentication mode to SN and password authentication.

always-on—— According to different authentication methods, the first authentication will use password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will not be automatically matched, and each subsequent authentication will use the same authentication method as the first

authentication. After the ONT is certified, it can go online even if the SN is modified.

once-on—— According to different authentication methods, the first authentication uses password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will be automatically matched, and each subsequent authentication will use the method of SN or SN+password/ SN+LOID / SN+LOID+password, which corresponds to the authentication method of the first authentication.

sn—— Configure the second and subsequent authentication to only verify the SN.

sn password—— Configure the second and subsequent authentication to verify the SN and password at the same time.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the auto-authentication mode of the ONT as password authentication:

```
Device(config-if-gpon)# ont auto-auth authmode password-auth
always-on
```

13.16 ont auto-auth rule

Description

The **ont auto-auth rule** command is used to add the auto-authentication rule of the ONT. The ONT which is auto-authenticated is bound with the specified line profile. To delete the rule, use **no ont auto-auth rule** command.

Syntax

ont auto-auth rule [*rule-id*] {equip-id *equip-id* | vendor-id *vendor-id* | version *version*} {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]} {[ont-srvprofile-id *profile-id]* | [ont-srvprofile-name *profile-name*] } [ont-mgmtprofile-id *profile-id* | ont-mgmtprofile-name *profile-name*]*

no ont auto-auth rule *rule-id*

Parameter

rule-id—— Specify the Rule number. This parameter is optional. If not specified, the system automatically assigns the smallest available Rule ID.

equip-id—— Set the value of the matching device ID, and the ONT that meets the matching rules can be automatically authenticated and registered.

vendor-id—— Set the value of the matching vendor ID, and the ONT that meets the matching rules can be automatically authenticated and registered.

version—— Set the value of the matching device software version, and the ONT that meets the matching rules can automatically authenticate and register.

ont-lineprofile-id—— The line profile ID.

ont-lineprofile-name—— The line profile name.

ont-srvprofile-id—— The service profile ID.

ont-srvprofile-name—— The service profile name.

ont-mgmtprofile-id—— The management profile ID.

ont-mgmtprofile-name—— The management profile name.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify rule1 to add the auto-authentication rule of the ONT. The ONT which is auto-authenticated is bound with the specified line profile:

```
Device(config-if-gpon)# ont auto-auth rule 1 equip-id

equip1ont-lineprofile-id 0 ont-srvprofile-id 0
```

13.17 show ont auto-auth

Description

The **show ont auth-info** command is used to display the auto-authentication information of ONTs. Sort by Rule ID in ascending order, and display the following information: Rule ID, Authentication method, Equip ID, Vendor ID, Software Version, Line profile, Service profile, and Management profile.

Syntax

show ont auto-auth [*pon-port-list*]

Parameter

pon-port-list—— The PON port list.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Displays the auto-authentication information of ONTs configured by 1/0/1:

```
Device(config)# show ont auto-auth 1/0/1
```

13.18 ont re-register

Description

The **ont re-register** command is used to reactivate the ONTs.

Syntax

ont re-register *ontid-list*

Parameter

ontid-list—— The ID list of the ONTs.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Reactivate the ONT 0:

```
Device(config-if-config)# ont re-register 0
```

13.19 ont reboot

Description

The **ont reboot** command is used to restart the ONTs.

Syntax

ont reboot *ontid-list*

Parameter

ontid-list—— The ID list of the ONTs.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Restart the ONT 0:

```
Device(config-if-config)# ont reboot 0
```

Chapter 14 ONU-Management Commands

After the ONU is authenticated and registered, you can manage the ONUs.

14.1 ont port attribute admin-status

Description

The **ont port attribute** command is used to enable or disable the specified ONT port.

Syntax

ont port attribute *ont-id* {eth *eth-port-id* | pots *pots-id*} **admin-status** {enable | disable}

Parameter

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

pots-id—— The ID of the ONT POTS port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the specified ONT ETH port:

```
Device(config-if-gpon)# ont port attribute 0 eth 1 admin-status enable
```

14.2 ont port native-vlan

Description

The **ont port native-vlan** command is used to configure the native VLAN for the uplink traffic of the ONT. To disable the native VLAN configuration, use **no ont port native-vlan** command.

Syntax

ont port native-vlan *ont-id* {eth *eth-port-id* | pots} {[vlan *vlan-id*] | [priority *priority*]}

no ont port native-vlan *ont-id* {eth *eth-port-id* | pots}

Parameter

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

vlan-id—— The ID of the native VLAN.

priority—— The priority of the native VLAN.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the native VLAN for the uplink traffic of the ONT to 1:

```
Device(config-if-gpon)# ont port native-vlan 0 eth 1 vlan 1
```

14.3 ont port attribute speed

Description

The **ont port attribute speed** command is used to configure the ONT port speed.

Syntax

ont port attribute *ont-id* **eth** *eth-port-id* **speed** *speed-val*

Parameter

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

speed-val—— The negotiation speed value of the ONT ETH port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ONT port speed to 10Mb/s:

```
Device(config-if-gpon)# ont port attribute 0 eth 1 speed 10
```

14.4 ont port attribute duplex

Description

The **ont port attribute duplex** command is used to configure the ONT port duplex mode.

Syntax

ont port attribute *ont-id* **eth** *eth-port-id* **duplex** {auto | full | half}

Parameter

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

auto—— The automatic mode of the ONT port.

full—— The full duplex mode of the ONT port.

half—— The half duplex mode of the ONT port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ONT port duplex mode to auto mode:

```
Device(config-if-gpon)# ont port attribute 0 eth 1 duplex auto
```

14.5 ont port attribute flow-control

Description

The **ont port attribute flow-control** command is used to enable the ONT port flow-control feature. To disable this feature, use **no ont port attribute flow-control**

Syntax

ont port attribute *ont-id* **eth** *eth-port-id* **flow-control**

no ont port attribute *ont-id* **eth** *eth-port-id* **flow-control**

Parameter

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ONT port flow-control feature:

```
Device(config-if-gpon)# ont port attribute 0 eth 1 flow-control
```

14.6 ont port car

Description

The **ont port car** command is used to bind the traffic profile to the ONT port to set the rate limit. To unbind the traffic profile, use **no ont port car** command**.**

Syntax

ont port car *ont-id* **eth** *eth-port-id traffic-profile-id*

no ont port car *ont-id* **eth** *eth-port-id*

Parameter

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

traffic-profile-id—— The traffic profile ID bound to the ONT port.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind the traffic profile to the ONT port to set the rate limit:

```
Device(config-if-gpon)# ont port car 0 eth 1 1
```

14.7 show ont port attribute

Description

The **show ont port attribute** command is used to display the information of ONT Ethernet ports in detail.

Syntax

show ont port attribute *pon-port-id ont-id* {eth {*eth-port-id* | all } | pots {*pots-id* | all} }

Parameter

pon-port-id—— The PON port list.

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

pots-id-list—— The ID list of the ONT POTS port.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of ONT Ethernet ports configured by 1/0/1 in detail:

```
Device(config)# show ont port attribute 1/0/1 0 eth 1
```

14.8 show ont port state

Description

The **show ont port state** command is used to display the status of ONT Ethernet ports in detail.

Syntax

show ont port state *pon-port-id ont-id* {eth {*eth-port-id* | all } | pots {*pots-id* | all} }

Parameter

pon-port-id—— The PON port list.

ont-id—— The ID of the ONT.

eth-port-id—— The ID of the ONT ETH port.

pots-id-list—— The ID list of the ONT POTS port.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the status of ONT Ethernet ports configured by 1/0/1 in detail.:

```
Device(config)# show ont port state 1/0/1 0 eth 1
```

14.9 ont wan

Description

The **ont wan** command is used to create or modify a new ONT WAN connection using the unique identification of ont-id and wan-id. If the wan-id corresponding to a specific ont-id does not exist, then create a new WAN connection. If the wan-id corresponding to a specific ont-id exists, then modify the existing WAN connection. To delete the ONT WAN connection, use **no ont wan** command**.**

Note: When the connection type is PPPoE, it is necessary to first create a wan-pppoeprofile and input the username and password for PPPoE dial-up.

The **batch** command is used for batch operations on WAN connections, and the **action push** command is used to simultaneously push the WAN connection to the ONU.

Syntax

The WAN Connection type is Bridge:

ont wan *ont-id wan-id* **admin-status** {enable | disable} **conn-type bridge** {internet | internet-tr069 | internet-voip | internet-voip-tr069 | other | tr069 | voip | voip-tr069} *mtu-val* [**vlan** *vlan-id* **priority** *priority*] [**lan-dhcp** {enable | disable}] [**conn-name** *name*] [**port-banding** {[**eth** *port_id_list*]|[**wifi_2_4_g**] |[**wifi_5g_1**] |[**wifi_5g_2**]}]

The WAN Connection type is Dynamic-IP:

ont wan *ont-id wan-id* **admin-status** {enable | disable} **conn-type dynamic-ip** {internet | internet-tr069 | internet-voip | internet-voip-tr069 | other | tr069 |voip | voip-tr069} *mtu-val* [**vlan** *vlan-id* **priority** *priority*] [**lan-dhcp** {enable |disable}] [**nat** {enable | disable}] [**conn-name** *name*] {[**ipv4 dns-type** {auto |manual } { [**primary-dns** i*pv4_addr*] |[**secondary-dns** *ipv4_addr*]}

[**ipv4-default-gateway** {enable | disable}]] | [**ipv6** {dhcpv6|slaac} **dns-type** {auto|manual} {[**ipv6-primary-dns** *ipv6_addr*] | [**ipv6-secondary-dns** *ipv6_addr*]} [**ipv6-default-gateway** {enable | disable}]} [**port-banding** {[**eth** *port_id_list*] |[**wifi_2_4_g**] | [**wifi_5g_1**] | [**wifi_5g_2**]}]

The WAN Connection type is PPPoE:

ont wan-pppoeprofile *ont-id wan-id*

pppoe-username *username*

pppoe-password *password*

ont wan *ont-id wan-id* **admin-status** {enable | disable} **conn-type pppoe** {internet | internet-tr069 | internet-voip | internet-voip-tr069 | other | tr069 | voip | voip-tr069} *mtu-val* [**vlan** *vlan-id* **priority** *priority*] [**nat** {enable | disable}] [**lan-dhcp** {enable | disable}] [**conn-name** name] {[**ipv4** [**ipv4-default-gateway** {enable|disble}]] | [**ipv6** {dhcpv6 | slaac} [**ipv6-default-gateway** {enable|disble}]]} [**port-banding** {[**eth** *port_id_list*] | [**wifi_2_4_g**] | [**wifi_5g_1**] | [**wifi_5g_2**]}]

The WAN Connection type is Static:

ont wan *ont-id wan-id* **admin-status** {enable | disable} **conn-type static**{internet | internet-tr069 | internet-voip | internet-voip-tr069 | other | tr069 |voip | voip-tr069} *mtu-val* [**nat** {enable | disable}] [**lan-dhcp** {enable | disable}][**conn-name** *name*] [**vlan** *vlan-id* **priority** *priority*] {[**ipv4** *Ipv4_addr ipv4_mask ipv4_gateway ipv4_pri_dns_addr* [**secondary-dns** *ipv4_sec_dns_addr*] [**ipv4-default-gateway** {enable|disble}]]| [**ipv6** *Ipv6_addr ipv6_prefix_length ipv6_gateway ipv6_pri_dns_addr* [**ipv6-secondary-dns** *ipv6_sec_dns_addr*] [**ipv6-default-gateway** {enable|disble}]]} [**port-banding** {**eth** [*port_id_list*] | [**wifi_2_4_g]** | [**wifi_5g_1]** | **[wifi_5g_2]**}]

ont wan { *ont-id wan-id* | batch *ontlist wanid-list* } **action push**

no ont wan { *ont-id wan-id* | batch *ontlist wanid-list* } [action push]

Parameter

ont-id—— The ID of the ONT.

wan-id—— The ID of the WAN connection.

ontlist—— The ID list of the ONT.

wanid-list—— The ID list of the WAN connection.

bridge—— The WAN connection type is bridge.

pppoe—— The WAN connection type is PPPOE.

dynamic-ip—— The WAN connection type is dynamic-ip.

static—— The WAN connection type is static.

auto—— Obtain DNS automatically.

manual—— To manually set DNS, you need to set primary-DNS and secondary-DNS.

primary-DNS—— Set the IP of the manually configured primary DNS Server.

secondary-DNS—— Set the IP of the manually configured secondary DNS server.

username—— The username used by PPPOE for dialing.

password—— The password used by PPPOE dial.

IPv4_addr—— The static IP address for IPv4.

IPv4_mask—— The static IP address mask for IPv4.

IPv4_gateway—— The gateway IP address for IPv4.

IPv4_pri_dns_addr—— The manually configured primary DNS Server IP address for IPv4.

IPv4_sec_dns_addr—— The manually configured secondary DNS Server IP address for IPv4.

IPv6_addr—— The static IP address for IPv6.

IPv6_mask—— The static IP address mask for IPv6.

IPv6_gateway—— The gateway IP address for IPv6.

IPv6_pri_dns_addr—— The manually configured primary DNS Server IP address for IPv6.

IPv6_sec_dns_addr—— The manually configured secondary DNS Server IP address for IPv6.

slaac—— Set the IPV6 addressing type to SLAAC.

dhcpv6—— Set the IPV6 addressing type to DHCPv6.

ipv4-default-gateway—— When the admin-status is enabled, set this connection as the default connection for IPv4.

ipv6-default-gateway—— When the admin-status is enabled, set this connection as the default connection for IPv6.

vlan-id—— Set the VLAN ID to which the WAN connection belongs.

priority—— Set the priority of the WAN connection.

Internet—— Indicates that the connection is used for the Internet.

Internet-tr069—— Indicates that the connection is used for Internet and TR069 services.

Internet-voip—— Indicates that the connection is used for Internet and voice services.

Internet-voip-tr069—— Indicates that the connection is used for Internet access, voice services and TR069 services.

other—— Indicates that the connection is for IPTV service.

tr069—— Indicates that the connection is used for TR069 service

voip—— Indicates that the connection is used for voice services.

voip-tr069—— Indicates that the connection is used for voice and TR069 services.

mtu-val—— Set MTU value.

lan-dhcp—— Enable or disable the DHCP function of the LAN port.

nat—— Enable or disable the NAT function of the WAN connection.

name——The name of the WAN connection.

port-id-list—— The value range of the ONT port bound to the WAN connection.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create or modify the WAN connection of the ONT in bridge mode:

```
Device(config-if-gpon)# ont wan 1 1 admin-status enable conn-type
bridge internet 64 vlan 1 priority 0
```

14.10 ont wan admin-status

Description

The **ont wan admin-status** command is used to enable or disable the ONT WAN connection.

Syntax

ont wan *ont-id wan-id* **admin-status** {enable | disable}

Parameter

ont-id—— The ID of the ONT.

wan-id—— The ID of the ONT WAN connection.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ONT WAN connection:

```
Device(config-if-gpon)# ont wan 0 1 admin-status enable
```

14.11 show ont wan

Description

The **show ont wan** command is used to display the information of the ONT WAN connection.

Syntax

show ont wan *pon-id ont-id* [*wan-id*]

Parameter

pon-id—— The ID of the ONT PON.

ont-id—— The ID of the ONT.

wan-id—— The ID of the ONT WAN connection.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the ONT WAN connection configured by 1/0/1:

```
Device(config)# show ont wan 1/0/1 0 1
```

14.12 ont upgrade

Description

The **ont upgrade** command is used to specify the FTP server for ONT upgrade.

Syntax

ont upgrade ftp *username password ip-addr filename*

Parameter

username—— The username for logging in to the FTP serve.

password—— The password for logging in to the FTP server.

ip-addr—— The IP address of the FTP server.

filename—— The name of the ONU image to be upgraded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the FTP server for ONT upgrade through the username "tplink", password "admin", and IP address "192.168.0.1":

```
Device(config)# ont upgrade ftp tplink admin 192.168.0.1 file1
```

14.13 ont upgrade ftp

Description

The **ont upgrade ftp** command is used to specify the FTP server for ONT upgrade.

Syntax

ont upgrade ftp *username password ip-addr*

Parameter

username —— The username for logging in to the FTP serve.

password —— The password for logging in to the FTP server.

ip-addr —— The IP address of the FTP server.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the FTP server for ONT upgrade through the username "tplink", password "admin", and IP address "192.168.0.1":

```
Device(config)# ont upgrade ftp tplink admin 192.168.0.1
```

14.14 ont upgrade filename

Description

The **ont upgrade filename** command is used to specify the filename for ONT upgrade.

Syntax

ont upgrade filename

Parameter

filename——The name of the ONU image to be upgraded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Use file1 as the fallback file for ONT upgrade:

```
Device(config)# ont upgrade filename file1
```

14.15 ont upgrade set

Description

The **ont upgrade set** command is used to set the ONT's upgrade config.

Syntax

ont upgrade set pon-port-list ont-id-list activemode {immediately | next-startup | schedule-time} filename schedule-time

Parameter

pon-port-list——The PON port list.

ont-id-list——The ID list of the ONT that need to be upgraded.

activemode——Specify the upgrade mode.

{

immediately——Restart and upgrade the ONT immediately.

next-start-up——Wait for the next restart of the ONT to start the upgrade.

schedule-time——Wait until the scheduled time is reached to start the upgrade.

}

filename——The filename used to upgrade the ONT.

schedule-time——The schedule time to be upgraded when the activemode is schedule-time.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure ONU 0–3 on GPON 1/1/1 to use the schedule-time upgrade mode, using file1 as the upgrade firmware, with the upgrade time set to 12:02 on May 1, 2026:

```
Device(config)# ont upgrade set gpon 1/1/1 0-3 activemode
schedule-time filename file1 schedule-time schedule-time
05/01/2026-12:02
```

14.16 ont upgrade stop

Description

The **ont upgrade stop** command is used to cancel the ONT's upgrade mission.

Syntax

ont upgrade stop *pon-port-list ont-id-list*

Parameter

pon-port-list——The PON port list.

ont-id-list——The ID list of the ONT that need to be stopped.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Cancel to upgrade mission of the ONT 0 in GPON 1/1/1:

```
Device(config)# ont upgrade stop gpon 1/1/1 0
```

14.17 show ont upgrade info

Description

The **show ont upgrade info** command is used to display the information of the ONT to be upgraded.

Syntax

show ont upgrade info

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

14.18 show ont upgrade progress

Description

The **show ont upgrade progress** command is used to display the progress of the ONT upgrade process.

Syntax

show ont upgrade progress

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

14.19 ont modify profile

Description

The **ont modify profile** command is used to modify the line or service profile which is bound with the ONT.

Syntax

ont modify *ont-id* {[ont-lineprofile-id *profile-id*] | [ont-lineprofile-name *profile-name*]}

ont modify *ont-id* {[ont-srvprofile-id *profile-id*] | [ont-srvprofile-name *profile-name*]}

ont modify *ont-id* {[ont-mgmtprofile-id *profile-id*] | [ont-mgmtprofile-name *profile-name*]}

Parameter

ont-id—— The ID of the ONT.

ont-lineprofile-id—— The line profile ID.

ont-lineprofile-name—— The line profile name.

ont-srvprofile-id—— The service profile ID.

ont-srvprofile-name—— The service profile name.

ont-mgmtprofile-id—— The management profile ID.

ont-mgmtprofile-name—— The management profile name.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Modify the line profile which is bound with the ONT:

```
Device(config-if-gpon)# ont modify 0 ont-lineprofile-id 0
```

14.20 ont modify authmode

Description

The **ont modify authmode** command is used to modify the authentication mode of the ONT.

Syntax

ont modify *ont-id* **authmode loid-and-password-auth** *loid-val loid-password* {always-on | once-on}

ont modify *ont-id* **authmode loid-auth** *loid-val* {always-on | once-on}

ont modify *ont-id* **authmode password-auth password-type** {asci | hex} *password-val* {always-on | once-on {sn | sn-password}}

ont modify *ont-id* **authmode sn-and-password-auth** *sn-val* **password-type** {asci | hex} *password-val*

ont modify *ont-id* **authmode sn-auth** *sn-val*

Parameter

ont-id—— The ID of the ONT.

loid-val—— The LOID value of the ONT.

loid-password—— The LOID password of the ONT.

password-type——The password type of the specified user.

password-val—— The password value of the ONT.

sn-val——— The SN value of the ONT.

always-on—— According to different authentication methods, the first authentication will use password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will not be automatically matched, and each subsequent authentication will use the same authentication method as the first authentication. After the ONT is certified, it can go online even if the SN is modified.

once-on—— According to different authentication methods, the first authentication uses password authentication / LOID authentication / LOID+password authentication. After the authentication is passed, the serial number will be automatically matched, and each subsequent authentication will use the method of SN or SN+password/ SN+LOID / SN+LOID+password, which corresponds to the authentication method of the first authentication.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Modify the authentication mode of the ONT to LOID value and LOID password authentication:

```
Device(config-if-gpon)# ont modify 0 authmode loid-and-password-auth
loid1 admin always-on
```

14.21 ont modify description

Description

The **ont modify description** command is used to modify the description of the ONT.

Syntax

ont modify *ont-id* **description** *desc*

Parameter

ont-id—— The ID of the ONT.

desc—— The description of the ONT.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Modify the description of the ONT:

```
Device(config-if-gpon)# ont modify 0 description description1
```

14.22 show ont capability

Description

The **show ont capability** command is used to display the port capability of the ONT.

Syntax

show ont capability *pon-port-list [ont-id-list]*

Parameter

pon-port-id-list—— The PON port list.

ont-id-list—— The ID list of the ONT.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port capability of the ONT configured by 1/0/1:

```
Device(config)# show ont capability 1/0/1 0
```

14.23 show ont config-capability

Description

The **show ont config-capability** command is used to display the configuration capability of the ONT.

Syntax

show ont config-capability *pon-port-id-list [ont-id-list]*

Parameter

pon-port-id-list—— The PON port list.

ont-id-list—— The ID list of the ONT.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration capability of the ONT configured by 1/0/1:

Device(config)# show ont config-capability 1/0/1 0

14.24 show ont failed-config

Description

The **show ont failed-config** command is used to display the failed configuration of the ONT.

Syntax

show ont failed-config *pon-id ont-id*

Parameter

pon-id—— The ID of the ONT PON port.

ont-id—— The ID of the ONT.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the failed configuration of the ONT configured by 1/0/1:

Device(config)# show ont failed-config 1/0/1 0

14.25 show ont info

Description

The **show ont info** command is used to display the authentication info of the ONT.

Syntax

show ont info {by-active-status {active|inactive}| by-match-status {match|mismatch}| by-online-status {online|offline}| by-admin-status {activated|deactivated} | by-config-status {success|failed}| by-desc *desc* | by-line-profile {profile-id *id* | profile-name *name*}| by-srv-profile {profile-id *id* | profile-name *name*} | by-mgmt-profile {profile-id *id* | profile-name *name*} | by-sn *sn-val* | gpon } *pon-port-list* [detail]

Parameter

by-active-status—— Display ONU information through active status.

by-match-status—— Display ONU information through match status.

by-online-status—— Display ONU information through online status.

by-admin-status—— Display ONU information through admin status.

by-config-status—— Display ONU information through config status.

by-desc—— Display ONU information through description.

by-line-profile—— Display ONU information through line profile.

by-srv-profile—— Display ONU information through service profile.

by-mgmt-profile—— Display ONU information through management profile.

by-sn—— Display ONU information through SN.

gpon—— Display ONU information through the PON port.

pon-port-list—— The PON port list.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the authentication info of the ONT configured by 1/0/1 by active-status:

```
Device(config)# show ont info by-active-status active 1/0/1
```

14.26 show ont optical-info

Description

The **show ont optical-info** command is used to display the optical line info of the ONT.

Syntax

show ont optical-info *pon-port-list [ont-id-list]*

Parameter

pon-port-list—— The PON port list.

ont-id-list—— The ID list of the ONT.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the optical line info of the ONT configured by 1/0/1:

```
Device(config)# show ont optical-info1/0/1 0
```

14.27 show ont version

Description

The **show ont version** command is used to display the version of the ONT.

Syntax

show ont version *pon-port-list [ont-id-list]*

Parameter

pon-port-list—— The PON port list.

ont-id-list—— The ID list of the ONT.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the version of the ONT configured by 1/0/1:

```
Device(config)# show ont version 1/0/1 0
```

14.28 show ont register-statistics

Description

The **show ont register-statistics** command is used to display the statistics of ONT registration.

Syntax

show ont register-statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics of ONT registration:

```
Device(config)# show ont register-statistics
```

14.29 ont iphost

Description

The **ont iphost** command is used to configure IPHOST on the ONT, which assigns IP addresses and related configurations to specific network hosts. With this command, IPHOST configurations can be pushed to the ONU device to expand the network and implement specific functionalities. The **no ont iphost** command is used to delete the configured IPHOST configurations.

Additionally, the **action push** directive is used to push the configurations to the ONU device for them to take effect, while the **batch** directive allows for batch pushing or deleting of IPHOST configurations, improving configuration efficiency.

Syntax

ont iphost *ontid ip-index* **dhcp** [vlan *vlanid* priority *priority*]

ont iphost *ontid ip-index* **static ip-address** *ip-address* **mask** *mask* [gateway *gateway* | primary-dns *primary-dns* | secondary-dns *secondary-dns* | vlan *vlanid* priority *priority*]*

no ont iphost {*ontid ip-index* | batch *ontlist ip-index-list*} [action push]

ont iphost {*ontid ip-index* | batch *ontlist ip-index-list*} **action push**

Parameter

ontid—— The ID number of the ONT. The value range is from 0 to 127.

ontlist—— The ONT ID list for batch operations. The value range is from 0 to 127,(e.g.:1-3, 5).

ip-index—— The index of the IP Host interface. The value range is from 1 to 2.

ip-index-list—— The index list of IP Hosts in batch configuration. The value range is from 1 to 2,(e.g.:1-2, 2).

ip-address—— The static IP address.

mask—— The address mask of the static IP address.

gateway—— The IP address of the gateway for the ONT management network.

primary-dns—— The IP address of the primary DNS server.

secondary-dns—— The IP address of the secondary DNS server.

vlanid—— The Management VLAN of the ONT. The value range is from 1 to 4094.

priority—— The Priority of the management VLAN on the ONT. The value range is from 0 to 7.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add IPHOST configurations on the ONT 1:

```
Device(config-if-gpon)# ont iphost 1 1 dhcp
```

14.30 show ont iphost

Description

The **show ont iphost** command is used to display the existing IPHOST configurations in the system.

Syntax

show ont iphost *portid ontid [ip-index]*

Parameter

portid—— The ID number of the PON port. It must be a valid PON port number.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

ip-index—— The index of the IP Host interface. The value range is from 1 to 2.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the IPHOST configured by 1/0/1:

```
Device(config)# show ont iphost 1/0/1 0
```

14.31 ont sipuser

Description

The **ont sipuser** command is used to add a SIP (Session Initiation Protocol) user account on the OLT. It enables the configuration of SIP user accounts to facilitate Voice over IP (VoIP) services. These user accounts allow for the initiation, modification, and termination of real-time voice and video communication sessions over the IP network. The **no ont sipuser** command is used to remove a specific SIP user account from the OLT configuration.

Additionally, the **action push** directive is used to push the configurations to the ONU device for them to take effect, while the **batch** directive allows for batch pushing or deleting of SIP configurations, improving configuration efficiency.

Syntax

ont sipuser *ontid sipuserid* **telno** *telno* **registration-server** *reg-server* [sipusername *sipusername* | sippassword *sippassword* | registration-port *port* | proxy-server *server* | proxy-port *port* | outbound-server *server* | outbound-port *port*]*

ont sipuser { *ontid sipuserid* | batch *ont-id-list sipuserid-list* } **action push**

no ont sipuser {*ontid sipuserid* | batch *ont-id-list sipuserid-list* } [action push]

Parameter

ontid—— The ID number of the ONT. The value range is from 0 to 127.

sipuserid—— The ID number of the SIP account. The value range is from 1 to 1.

ont-id-list—— The ID number list of the ONT. The value range is from 1 to 1.

sipuserid-list—— The ID number list of the SIP account. The value range is from 0 to 127.

telno—— The phone number of the SIP account. The length range is from 3 to 32.

sipusername—— The username of the SIP account. The length range is from 0 to 50.

sippassword—— The password of the SIP account. The length range is from 0 to 25.

reg-server—— The registrar server address of the ONT. The length range is from 1 to 40.

server—— The server of the ONT. The length range is from 0 to 40.

port—— The port of the ONT. The value range is from 0 to 65535.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a SIP account on the OLT:

```
Device(config-if-gpon)# ont sipuser 0 1 telno 123 registration-server 456
```

14.32 show ont sipuser

Description

The **show ont sipuser** command is used to display the existing SIP users in the system.

Syntax

show ont sipuser *portid ontid*

Parameter

portid—— The ID number of the PON port. It must be a valid PON port number.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the SIP user by 1/0/1:

Device(config)# show ont sipuser 1/0/1 0

14.33 ont wlan

Description

The **ont wlan** command is used to add WLAN (Wireless Local Area Network) configuration on the ONT. It allows for the configuration of Wi-Fi networks on the ONT, enabling wireless network connectivity. This command can be used to set parameters for the wireless network, such as the SSID (Service Set Identifier), encryption method, frequency band, etc., allowing terminal devices to connect to the network wirelessly. On the other hand, the **no ont wlan** command is used to delete the configured WLAN configuration, clearing out any unwanted wireless network settings.

Additionally, the **action push** directive is used to push the configurations to the ONU device for them to take effect, while the **batch** directive allows for batch pushing or deleting of WLAN configurations, improving configuration efficiency.

Syntax

ont wlan *ontid* {2_4g 2_4g_ssid *ssid* [2_4g_hide_ssid {enable | disable} | 2_4g_security *security* | 2_4g_password *password* | 2_4g_mode *mode* | 2_4g_channel *channel* | 2_4g_channel_width *width* | 2_4g_radio {enable | disable}] * | 5g_ 5g_ssid *ssid* [5g_hide_ssid {enable | disable} | 5g_security *security* | 5g_password *password* | 5g_mode *mode* | 5g_channel *channel* | 5g_channel_width *width* | 5g_radio {enable | disable}]* }*

ont wlan *ontid* **band-steering ssid** *ssid* [security *security* | ssid-password *password* | hide-ssid {enable | disable} | radio {enable | disable}]*

no ont wlan {*ontid* | batch *ontid-list*}

ont wlan *ontid* {*ontid* | batch *ontid-list*} **action push**

Parameter

ontid—— The ID number of the ONT. The value range is from 0 to 127.

ont-id-list—— The ID number list of the ONT. The value range is from 0 to 127.

ssid——The SSID of the WLAN. The length can range from 1 to 32 characters.

security——The encryption method of the WLAN. The valid values are: no_security, wpa_psk_tkip_wpa2_psk_aes, wpa2_psk_aes, wpa2_psk_aes_wpa3_personal

password——The password of the WLAN. The length can range from 8 to 63 characters. When the security is set to no_security, this parameter is not applicable.

mode——The mode of the WLAN. The 2.4G valid values are: 802_11_n, 802_11_g_n, 802_11_b_g_n; the 5G valid values are: 802_11_ac, 802_11_ac_n, 802_11_a_n_ac.

channel——The frequency band of the WLAN. The 2.4G valid values are: auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13; the 5G valid values are: auto, 36, 40, 44, 48, 149, 153,157,161.

width——The frequency band width of the WLAN. The 2.4G valid values are: auto, 20, 40; the 5G valid values are: auto, 20, 40, 80.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add an SIP account in the management profile:

```
Device(config-if-gpom)# ont wlan 0 2_4g 2_4g_ssid TP-Link_1234
```

14.34 show ont wlan

Description

The **show ont wlan** command is used to display the existing wlan configurations in the system.

Syntax

show ont wlan *portid ontid*

Parameter

portid—— The ID number of the PON port. It must be a valid PON port number.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the SIP user by 1/0/1:

```
Device# show ont wlan 1/0/1 0
```

14.35 ont catv

Description

The **ont catv** command is used to configure CATV parameters on the OLT. With this command, the fiber network administrator can set a series of parameters to support the transmission and reception of CATV signals over fiber, ensuring stable transmission of CATV signals and enabling end users to watch TV programs through related devices. The **no ont catv** command is used to delete the configured CATV configuration.

Additionally, the **action push** directive is used to push the configurations to the ONU device for them to take effect, while the **batch** directive allows for batch pushing or deleting of CATV configurations, improving configuration efficiency.

Syntax

ont catv *ontid* {enable | disable}

no ont catv {*ontid* | batch *ontid-list*}

ont catv {*ontid* | batch *ontid-list*} **action push**

Parameter

portid—— The ID number of the PON port. It must be a valid PON port number.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

ont-id-list—— The ID number list of the ONT. The value range is from 0 to 127.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add CATV configuration:

```
Device(config-if-gpon)# ont catv 0 enble
```

14.36 show ont catv

Description

The **show ont catv** command is used to display the existing catv information in the system.

Syntax

show ont catv *portid ontid*

Parameter

portid—— The ID number of the PON port. It must be a valid PON port number.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the SIP user by 1/0/1:

```
Device# show ont catv 1/0/1 0
```

14.37 ont cwmp

Description

The **ont cwmp** command is specifically used on the ONT to add the necessary configuration for enabling CPE WAN Management Protocol (CWMP). CWMP is a widely-used protocol that facilitates efficient remote management and configuration of customer premises equipment (CPE) in a wide area network (WAN) environment. With the ont cwmp command, the ONT can be configured to seamlessly integrate into a remote management system through CWMP, allowing network administrators to remotely manage and configure the ONT for optimal performance and troubleshooting. The **no ont cwmp** command is used to delete the configured CWMP configuration.

Additionally, the **action push** directive is used to push the configurations to the ONU device for them to take effect, while the **batch** directive allows for batch pushing or deleting of CWMP configurations, improving configuration efficiency.

Syntax

ont cwmp *ontid* **url** *acs-url* [username *acs-username* | pwd *acs-pwd* | cwmp-status {enable | disable} | inform-status{enable | disable} | inform-interval *inform-interval* | auth-status{enable | disable}]*

no ont cwmp {*ontid* | batch *ontlist*}

ont cwmp {*ontid* | batch *ontlist*} **action push**

Parameter

acs-url——The address of the ACS URL. The length can range from 1 to 255 characters.

acs-username——The username of the ACS URL. The length can range from 0 to 50 characters.

acs-pwd——The password of the ACS URL. The length can range from 0 to 25 characters.

inform-interval——The interval of inform messages. The value ranges from 1 to 4294967295.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

ont-id-list—— The ID number list of the ONT. The value range is from 0 to 127.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add CWMP configuration:

Device(config-if-gpon)# ont cwmp 0 **url** 192.168.1.1 **username** TP-Link **pwd** admin

14.38 ont cwmp-auth-profile

Description

The **ont cwmp-auth-profile** command is used to add a CWMP authentication profile on the ONT. When configuring CWMP, if the auth-status is set to enable, it will bind to this profile.

Syntax

ont cwmp-auth-profile *ontid*

conn-auth path *path* **port** *port*

auth-username *auth-username*

auth-password *auth-password*

Parameter

ontid—— The ID number of the ONT. The value range is from 0 to 127.

path——The path of the authentication. The length can range from 1 to 15 characters and must start with a "/".

port——The port of the authentication. The interval of inform messages. The value ranges from 1000 to 65535.

auth-username——The username of the authentication. The length can range from 0 to 255 characters.

auth-password——The password of the authentication. The length can range from 0 to 255 characters.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a CWMP authentication profile:

```
Device(config-if-gpon)# ont cwmp-auth-profile 0
Device(config-ont-cwmp-auth)# conn-auth path /192.168.1.1 port 1000
```

14.39 show ont cwmp

Description

The **show ont cwmp** command is used to display the existing cwmp configurations in the system.

Syntax

show ont cwmp *portid ontid*

Parameter

portid—— The ID number of the PON port. It must be a valid PON port number.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the cwmp configuration by 1/0/1:

```
Device(config)# show ont cwmp 1/0/1 0
```

14.40 ont isolation

Description

The **ont isolation** command is specifically used to configure the VLAN-based ONT isolation feature. With this feature, individual ONTs (Optical Network Terminals) can be isolated from each other by assigning them to separate

VLANs. This allows for enhanced network security and segmentation, as traffic from different ONTs can be kept separate. The ont isolation command enables network administrators to enable and configure this feature on the ONT, ensuring that each ONT operates within its designated VLAN. The **no ont isolation** command is used to delete the configured isolation configuration.

Syntax

ont isolation

no ont isolation

ont isolation vlan *vlanid-list*

no ont isolation vlan *vlanid-list*

Parameter

vlanid-list—— The VLAN list of the ONT. The value range is from 1 to 4094, (e.g., 1-100, 4094).

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure VLAN-based ONT isolation feature:

```
Device(config)# ont isolation vlan 1-3, 5
```

14.41 show ont isolation

Description

The **show ont isolation** command is used to display the existing ONT isolation configurations in the system.

Syntax

show ont isolation

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the existing ONT isolation configurations:

```
Device(config)# show ont isolation
```

14.42 show ont learned-mac

Description

The **show ont learned** command is used to display the existing client mac of ONT.

Syntax

show ont learned *pon-port-id ont-id ont-port-type ont-port-id*

Parameter

pon-port-id——The ID number of the PON port. It must be a valid PON port number.

ont-id—— The ID number of the ONT. The value range is from 0 to 127 for GPON port and 0 to 255 for XGSPON port.

ont-port-type——The type of ONT port, could be eth and wlan.

ont-port-id——The Id number of the ONT eth port or the type of the wlan.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the client MAC of eth 1 for ONU 0 under GPON 1/1/1:

```
Device(config)# show ont learned-mac gpon 1/1/1 0 eth 1
```

14.43 ont remote-access

Description

The **ont remote-access** command is used to manage the remote-access configuration on the ONT. The **no ont remote-access** command is used to clear the configuration.

Syntax

ont remote-access *ontid* {*enable* | *disable*}

no ont remote-access {*ontid* | batch *ontid-list*}

ont remote-access {*ontid* | batch *ontid-list*} **action push**

Parameter

ontid —— The ID number of the ONT. The value range is from 0 to 127.

ontid-list —— The ID number list of the ONT. The value range is from 0 to 127.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the remote-access configuration on the ONT 1:

```
Device(config)# interface gpon 1/1/1
Device(config-if-gpon)# ont remote-access 1 enable
```

14.44 show ont remote-access

Description

The **show ont remote-access** command is used to display the existing remote-access information in the system.

Note: Detailed syntax and required parameters may vary depending on the specific OLT product.

Syntax

show ont remote-access gpon *portid ontid*

Parameter

portid—— The ID number of the PON port. It must be a valid PON port number.

ontid—— The ID number of the ONT. The value range is from 0 to 127.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the existing remote-access information in the system:

Device# show ont remote-access gpon 1/0/1 1

Chapter 15 Service Port Configuration Commands

Service ports are used by OLT to map different types of traffic to different SVLANs according to PON ports, ONUs, GEM ports, User VLANs, and priorities, and then transmitted to the uplink network. The rate limit for inbound and outbound traffic of the uplink network is determined by traffic profiles which are applied to the service ports.

15.1 service-port

Description

The **service-port** command is used to create a service port. To delete the service port or delete some configurations of the service port, use **no service-port** command.

Syntax

service-port {servicePortId | auto} { adminstatus {enable | disable} | description *description* | inbound-traffic *trafficProfileId* | outbound-traffic *trafficProfileId* | statistics-performance {enable | disable} | config gpon *ponPortId* ont *ontIdList* gem-id *gemId* svlan *svlanId* [user-vlan *vlanId* | user-pri *vlanPri* | ethertype {none | ipv4oe | ipv6oe | pppoe} | tag-action {default | transparent | translate | translate-add | add-double} | inner-vlan *vlanId* | inner-pri *vlanPri* | traffic-in *trafficProfileId* | traffic-out *trafficProfileId* | desc *description* | adminstatus {enable | disable} | statistic-performance {enable | disable}] }

Parameter

servicePortId|auto—— The port ID of the service port.

inbound-traffic—— Modify the traffic profile to be called in the upstream direction after the service-port matches the data flow.

outbound-traffic—— Modify the traffic profile to be called in the downstream direction after the service-port matches the data flow.

description—— Modify the item description of the service port.

adminstatus—— Modify the enabled status of the service flow matched by the service port.

statistics-performance —— Modify the traffic statistics switch status of the service flow matched by the service port.

config—— Create or modify the service port. If the service port does not exist, create it. If the service port already exists, use the new configuration to

overwrite the original configuration. At this time, it can be regarded as modifying the original configuration.

gpon—— Specify which pon port the service port is applied to.

ont —— Specify which onts the service port is applied to.

gem-id —— Specify which gem of the ont the service port is applied to.

svlan—— Specify the svlan of the service port.

user-vlan—— Specify the user-vlan of the data flow matched by the service port.

user-pri —— Specify the user-pri of the data flow matched by the service port.

ethertype—— Specify the data flow packet type matched by the service port.

tag-action—— Specify the action performed by the service port on the matched data stream.

default: Add a layer of SVLAN, and the CVLAN carried on the user side remains unchanged.

transparent: Directly use the user-side CVLAN as the SVLAN to upstream.

translate: Translate the CVLAN carried by the user side into the specified SVLAN.

translate-add: Switch the CVLAN carried by the user to the newly configured Inner VLAN, and add a layer of SVLAN.

add-double: add two VLANs to the message, SVLAN+Inner VLAN.

inner-vlan —— When the specified action for the matched data stream is translate-add/add-double, the added inner vlan needs to be specified.

inner-pri—— When the specified action for the matched data stream is translate-add/add-double, you need to specify the priority of the added inner VLAN.

traffic-in—— Specify the traffic profile to be invoked in the upstream direction after the service-port matches the data flow.

traffic-out—— Specify the traffic profile to be called in the downstream direction after the service-port matches the data flow

desc—— Specify the item description of the service port.

adminstatus—— Specify the enabled status of the service flow matched by the service port.

statistic-performance—— Specify the traffic statistics switch status of the service flow matched by the service port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Modify the service flow state matching the service port 1 to enable:

```
Device(config)# service-port 1 adminstatus enable
```

15.2 show service-port

Description

The **show service-port** command is used to display the service port info.

Syntax

show service-port {*servicePortId* [statistics] | ethertype | gpon | svlan | user-vlan }

Parameter

servicePortId—— Display the service port of the specified id.

statistics—— Display statistics of the specified service port.

ethertype—— Display all service ports of the specified ethertype.

gpon—— Display all service ports of the specified gpon port.

svlan—— Display all service ports of the specified svlan.

user-vlan—— Display all service ports of the specified user-vlan.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the service-port 1 information:

```
Device(config)# show service-port 1
```

15.3 auto-service-port

Description

The **auto-service-port** command is used to create an auto service port. To delete some configurations of the auto service port, use **no auto-service-port** command.

Syntax

auto-service-port { auto-mode {*enable|disable*} | inbound-traffic *trafficProfileId* | outbound-traffic *trafficProfileId* | config gem-id *gemId* svlan *svlanId* [user-vlan *vlanId* | user-pri *vlanPri* | ethertype {*none | ipv4oe | ipv6oe | pppoe*} | tag-action {*default | transparent | translate | translate-add | add-double*} | inner-vlan *vlanId* | inner-pri *vlanPri* | traffic-in *trafficProfileId* | traffic-out *trafficProfileId* | auto-mode {*enable | disable*}] }

no auto-service-port { inbound-traffic | outbound-traffic }

Parameter

gpon—— Specify the auto service port of a port to be operated.

auto-mode—— Modify the switch state of the port automatic flow creation function.

inbound-traffic—— Modify the traffic profile to be called in the upstream direction after the service-port matches the data flow.

outbound-traffic—— Modify the traffic profile to be called in the downstream direction after the service-port matches the data flow.

config—— Modify more detailed configuration of auto service port.

gem-id—— Specify which gem of the ont the service port is applied to.

svlan—— Specify the svlan of the service port.

user-vlan—— Specify the user-vlan of the data flow matched by the service port.

user-pri—— Specify the user-pri of the data flow matched by the service port.

ethertype—— Specify the data flow packet type matched by the service port.

tag-action—— Specify the action performed by the service port on the matched data stream.

default: Add a layer of SVLAN, and the CVLAN carried on the user side remains unchanged.

transparent: Directly use the user-side CVLAN as the SVLAN to upstream.

translate: Translate the CVLAN carried by the user side into the specified SVLAN.

translate-add: Switch the CVLAN carried by the user to the newly configured Inner VLAN, and add a layer of SVLAN.

add-double: add two VLANs to the message, SVLAN+Inner VLAN.

inner-vlan—— When the specified action for the matched data stream is translate-add/add-double, the added inner vlan needs to be specified.

inner-pri—— When the specified action for the matched data stream is translate-add/add-double, you need to specify the priority of the added inner VLAN.

traffic-in—— Specify the traffic profile to be invoked in the upstream direction after the service-port matches the data flow.

traffic-out—— Specify the traffic profile to be called in the downstream direction after the service-port matches the data flow.

auto-mode—— Modify the switch state of the port automatic flow creation function.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Modify the switch status of the automatic flow creation function of automatic service port 1/0/1 to enable:

Device(config)# auto-service-port interface gpon 1/0/1 **auto-mode enable**

15.4 show auto-service-port

Description

The **show auto-service-port** command is used to display the auto service port info.

Syntax

show auto-service-port interface gpon *ponPortId*

Parameter

ponPortId—— Display the auto service port of the specified port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the auto service port 1/0/1 information:

```
Device(config)# show auto-service-port interface gpon 1/0/1
```

Chapter 16 Ethernet Port Configuration Commands

Ethernet Configuration Commands can be used to configure the Negotiation Mode for Ethernet ports.

16.1 interface gigabitEthernet

Description

The **interface gigabitEthernet** command is used to enter the Interface gigabitEthernet Configuration Mode and configure the corresponding Gigabit Ethernet port.

Syntax

interface gigabitEthernet *port*

Parameter

port —— The Ethernet port number.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

To enter the Interface gigabitEthernet Configuration Mode and configure port 2:

```
Device(config)# interface gigabitEthernet 1/0/2
```

16.2 interface range gigabitEthernet

Description

The **interface range gigabitEthernet** command is used to enter the interface range gigabitEthernet Configuration Mode and configure multiple Gigabit Ethernet ports at the same time.

Syntax

interface range gigabitEthernet *port-list*

Parameter

port-list —— The list of Ethernet ports.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Command in the **Interface Range gigabitEthernet** Mode is executed independently on all ports in the range. It does not affect the execution on the other ports at all if the command results in an error on one port.

Example

To enter the Interface range gigabitEthernet Configuration Mode, and configure ports 1, 2, 3, 6, 7 and 9 at the same time by adding them to one port-list:

Device(config)# interface range gigabitEthernet 1/0/1-3,1/0/6-7,1/0/9

16.3 description

Description

The **description** command is used to add a description to the Ethernet port. To clear the description of the corresponding port, please use **no description** command.

Syntax

description *string*

no description

Parameter

string —— Content of a port description, ranging from 1 to 16 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a description Port_5 to port 1/0/5:

Device(config)# interface gigabitEthernet 1/0/5

Device(config-if)# description Port_5

16.4 shutdown

Description

The **shutdown** command is used to disable an Ethernet port. To enable this port again, please use **no shutdown** command.

Syntax

shutdown

no shutdown

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# shutdown

16.5 flow-control

Description

The **flow-control** command is used to enable the flow-control function for a port. To disable the flow-control function for this corresponding port, please use **no flow-control** command. With the flow-control function enabled, the Ingress Rate and Egress Rate can be synchronized to avoid packet loss in the network.

Syntax

flow-control

no flow-control

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the flow-control function for port 1/0/3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# flow-control
```

16.6 fec-mode

Description

The **fec-mode** command is used to configure the FEC (Forward Error Correction) mode for an interface. FEC is used to enhance transmission reliability on high-speed links in scenarios with bit errors.

Syntax

fec-mode { none | auto | cl91 }

Parameters

None —— No FEC enabled.

auto —— The FEC mode is automatically selected according to the transceiver type.

cl91 —— Enables IEEE 802.3 RS-FEC(528, 514) (Clause 91).

Command Mode

Interface Configuration Mode

Privilege Requirement

None

Example

Enable the fec mode:

```
Device(config-if)# fec-mode auto
```

16.7 duplex

Description

The **duplex** command is used to configure the Duplex Mode for an Ethernet port. To return to the default configuration, please use **no duplex** command.

Syntax

duplex { auto | full | half }

no duplex

Parameter

auto | full | half —— The duplex mode of the Ethernet port. There are three options: auto-negotiation mode, full-duplex mode and half-duplex mode. By default, the Gigabit Ethernet port is auto-negotiation mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the Duplex Mode as full-duplex for port 1/0/3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# duplex full
```

16.8 jumbo-size

Description

The **jumbo-size** command is used to specify the size of jumbo frames.

Syntax

jumbo-size *size*

Parameter

size —— The value of jumbo frames. It ranges from 1518 to 9216 bytes, and the default is 1518 bytes.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Globally configure the size of jumbo frames as 9216:

```
Device(config)# jumbo-size 9216
```

16.9 speed

Description

The **speed** command is used to configure the Speed Mode for an Ethernet port. To return to the default configuration, please use **no speed** command.

Syntax

speed { 10 | 100 | 1000 | auto }

no speed

Parameter

10 | 100 | 1000 | auto —— The speed mode of the Ethernet port. There are four options: 10Mbps, 100Mbps, 1000Mbps and Auto negotiation mode (default).

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the Speed Mode as 100Mbps for port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# speed 100

16.10 clear counters

Description

The **clear counters** command is used to clear the statistics information of all the Ethernet ports and port channels.

Syntax

clear counters

clear counters interface [gigabitEthernet *port*] [port-channel *port-channel-id*]

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Clear the statistic information of all ports and port channels:

Device(config)# clear counters

16.11 show fiber-ports

Note: This command is only available on certain devices.

Description

The **show fiber-ports** command is used to display the information of all fiber ports.

Syntax

show fiber-ports

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all fiber ports:

```
Device(config)# show fiber ports
```

16.12 show interface status

Description

The **show interface status** command is used to display the connection status of the Ethernet port/port channel.

Syntax

show interface status [fastEthernet *port*] [gigabitEthernet *port*] [ten-gigabitEthernet *port*] [port-channel *port-channel-id*]

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel..

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the connection status of all ports and port channels:

```
Device(config)# show interface status
```

Display the connection status of port 1/0/1:

```
Device(config)# show interface status gigabitEthernet 1/0/1
```

16.13 show interface counters

Description

The **show interface counters** command is used to display the statistics information of all ports/port channels.

Syntax

show interface counters [gigabitEthernet *port*] [port-channel *port-channel-id*]

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics information of all Ethernet ports and port channels:

```
Device(config)# show interface counters
```

Display the statistics information of port 1/0/2:

```
Device(config)# show interface counters gigabitEthernet 1/0/2
```

16.14 show interface configuration

Description

The **show interface configuration** command is used to display the configurations of all ports and port channels, including Port-status, Flow Control, Negotiation Mode and Port-description.

Syntax

show interface configuration [gigabitEthernet *port*] [port-channel *port-channel-id*]

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of all Ethernet ports and port channels:

Device(config)# show interface configuration

Display the configurations of port 1/0/2:

Device(config)# show interface configuration gigabitEthernet 1/0/2

Chapter 17 Port Isolation Commands

Port Isolation provides a method of restricting traffic flow to improve the network security by forbidding the port to forward packets to the ports that are not on its forwarding port list.

17.1 port isolation

Description

The **port isolation** command is used to configure the forward port/port channel list of a port/port channel, so that this port/port channel can only communicate with the ports/port channels on its list. To delete the corresponding configuration, please use **no port isolation** command.

Syntax

port isolation { [fa-forward-list *fa-forward-list*] [gi-forward-list *gi-forward-list*] [po-forward-list *po-forward-list*] [te-forward-list *te-forward-list*] }

no port isolation

Parameter

fa-forward-list / *gi-forward-list* / *te-forward-list* —— The list of Ethernet ports.

po-forward-list —— The list of port channels.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set port 1, 2, 4 and port channel 2 to the forward list of port 1/0/5:

```
Device(config)# interface gigabitEthernet 1/0/5
Device(config-if)# port isolation gi-forward-list 1/0/1-2,1/0/4
po-forward-list 2
```

Set all Ethernet ports and port channels to forward list of port 1/0/2, namely restore to the default setting:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# no port isolation
```

17.2 show port isolation interface

Description

The **show port isolation interface** command is used to display the forward port list of a port/port channel.

Syntax

show port isolation interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port ——The number of Ethernet port you want to show its forward port list, in the format of 1/0/2.

port-channel-id ——The ID of port channel you want to show its forward port list, ranging from 1 to 6.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the forward-list of port 1/0/2:

```
Device# show port isolation interface gigabitEthernet 1/0/2
```

Display the forward-list of all Ethernet ports and port channels:

```
Device# show port isolation interface
```

Chapter 18 Loopback Detection Commands

With loopback detection feature enabled, the device can detect loops using loopback detection packets. When a loop is detected, the device will display an alert or further block the corresponding port according to the configuration.

18.1 loopback-detection (global)

Description

The **loopback-detection** command is used to enable the loopback detection function globally. To disable it, please use **no loopback detection** command.

Syntax

loopback-detection

no loopback-detection

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the loopback detection function globally:

```
Device(config)# loopback-detection
```

18.2 loopback-detection interval

Description

The **loopback-detection interval** command is used to define the interval of sending loopback detection packets from device ports to network, aiming at detecting network loops periodically.

Syntax

loopback-detection interval *interval-time*

Parameter

interval-time —— The interval of sending loopback detection packets. It ranges from 1 to 1000 seconds. By default, this value is 30.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the interval-time as 50 seconds:

```
Device(config)# loopback-detection interval 50
```

18.3 loopback-detection recovery-time

Description

The **loopback-detection recovery-time** command is used to configure the time after which the blocked port would automatically recover to normal status.

Syntax

loopback-detection recovery-time *recovery-time*

Parameter

recovery-time —— The time after which the blocked port would automatically recover to normal status, and the loopback detection would restart. It ranges from 2 to 1000000 seconds. By default, this value is 90.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the recovery-time as 70 seconds:

```
Device(config)# loopback-detection recovery-time 70
```

18.4 loopback-detection (interface)

Description

The **loopback-detection** command is used to enable the loopback detection function of the specified port. To disable it, please use **no loopback-detection** command.

Syntax

loopback-detection

no loopback-detection

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the loopback detection function of ports 1-3:

```
Device(config)# interface range gigabitEthernet 1/0/1-3
Device(Config-if-range)# loopback-detection
```

18.5 loopback-detection config process-mode

Description

The **loopback-detection config process-mode** command is used to configure the process-mode for the ports by which the device copes with the detected loops. You also need to configure the recovery mode to remove the block status of the port or VLAN when the process-mode is Port Based or VLAN Based.

Syntax

loopback-detection config process-mode { alert | port-based | vlan-based } **recovery-mode** { auto | manual }

Parameter

alert —— When a loop is detected, the device will send a trap message and generate an entry on the log file. It is the default setting.

port-based —— When a loop is detected, the device will send a trap message and generate an entry on the log file. In addition, the device will block the port

on which the loop is detected and no packets can pass through the port.

vlan-based —— When a loop is detected, the device will send a trap message and generate an entry on the log file. In addition, the device will block the VLAN in which the loop is detected and only the packets of the blocked VLAN cannot pass through the port.

auto —— Block status can be automatically removed after recovery time.

manual —— Block status can only be removed manually.

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the loopback detection process-mode as port-based, and configure the recovery mode as manual for port 2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# loopback-detection config process-mode port-based

recovery-mode manual

18.6 loopback-detection recover

Description

The **loopback-detection recover** command is used to remove the block status of selected ports, recovering the blocked ports to normal status,

Syntax

loopback-detection recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Recover the blocked port 1/0/2 to normal status:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# loopback-detection recover
```

18.7 show loopback-detection global

Description

The **show loopback-detection global** command is used to display the global configuration of loopback detection function such as loopback detection global status, loopback detection interval and loopback detection recovery time.

Syntax

show loopback-detection global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of loopback detection function:

```
Device# show loopback-detection global
```

18.8 show loopback-detection interface

Description

The **show loopback-detection interface** command is used to display the configuration of loopback detection function and the status of the specified Ethernet port.

Syntax

show loopback-detection interface [gigabitEthernet *port* | port-channel *lagid*] [detail]

Parameter

port —— The Ethernet port number.

lagid —— The number of LAG, ranging from 1 to 32+.

detail —— Displays the loop status and block status of the VLAN which the specified port belongs to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of loopback detection function and the status of all ports:

Device# show loopback-detection interface

Display the configuration of loopback detection function and the status of port 5:

Device# show loopback-detection interface gigabitEthernet 1/0/5

Chapter 19 DDM Commands

The DDM (Digital Diagnostic Monitoring) function allows the user to monitor the status of the SFP modules inserted into the SFP ports on the device. The user can choose to shut down the monitoring SFP port automatically when specified parameter exceeds the alarm threshold or warning threshold. The monitoring parameters include: Temperature, Voltage, Bias Current, Tx Power and Rx Power.

19.1 ddm state enable

Description

The **ddm state enable** command is used to enable the DDM function on the specified SFP port.

Use the **no ddm state enable** command to disable the DDM function on this port.

Syntax

ddm state enable

no ddm state enable

Default Setting

Enabled on all the SFP ports.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Enable DDM function on port 1/0/25:

```
Device(config)#interface gigabitEthernet 1/0/25
Device(config-if)#ddm state enable
```

19.2 ddm shutdown

Description

The **ddm shutdown** command is used to configure whether to shut down the port when an exceeding alarm threshold or warning threshold event is encountered.

Syntax

ddm shutdown { none | warning | alarm }

Parameter

none —— The port will never be shut down regardless of the exceeding alarm threshold and warning threshold events.

warning —— Shut down the port when an exceeding warning threshold event is encountered.

alarm —— Shut down the port when an exceeding alarm threshold event is encountered.

Default Setting

none, which means the port will never be shut down regardless of the exceeding alarm threshold and warning threshold events.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Shut down the port 1/0/25 when an exceeding warning threshold event is encountered:

```
Device(config)#interface gigabitEthernet 1/0/25
Device(config-if)#ddm shutdown warning
```

19.3 ddm temperature_threshold

Description

The **ddm temperature_threshold** command is used to configure the threshold of the DDM temperature value.

Syntax

ddm temperature_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in Celsius.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM temperature on the port 1/0/25 as 5:

Device(config)#interface gigabitEthernet 1/0/25

Device(config-if)#ddm temperature_threshold high_alarm 5

19.4 ddm voltage_threshold

Description

The **ddm voltage_threshold** command is used to configure the threshold of the DDM voltage value.

Syntax

ddm voltage_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in Volt.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM voltage on the port 1/0/25 as 5:

Device(config)#interface gigabitEthernet 1/0/25

Device(config-if)#ddm voltage_threshold high_alarm 5

19.5 ddm bias_current_threshold

Description

The **ddm bias_current_threshold** command is used to configure the threshold of the DDM Bias Current value.

Syntax

ddm bias_current_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in mA.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Bias Current on the port 1/0/25 as 5:

```
Device(config)#interface gigabitEthernet 1/0/25
Device(config-if)#ddm bias_current_threshold high_alarm 5
```

19.6 ddm tx_power_threshold

Description

The **ddm tx_power_threshold** command is used to configure the threshold of the DDM Tx Power value.

Syntax

ddm tx_power_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in mW.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Tx Power on the port 1/0/25 as 5:

Device(config)#interface gigabitEthernet 1/0/25

Device(config-if)#ddm tx_power_threshold high_alarm 5

19.7 ddm rx_power_threshold

Description

The **ddm rx_power_threshold** command is used to configure the threshold of the DDM Rx Power value.

Syntax

ddm rx_power_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in mW.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Rx Power on the port 1/0/25 as 5:

Device(config)#interface gigabitEthernet 1/0/25

Device(config-if)#ddm rx_power_threshold high_alarm 5

19.8 show ddm configuration

Description

The **show ddm configuration** command is used to display the DDM configuration.

Syntax

show ddm configuration { state | temperature | voltage | bias_current | tx_power | rx_power }

Parameter

state —— Display the DDM configuration state.

temperature —— Displays the threshold of the DDM temperature value.

voltage —— Displays the threshold of the DDM Voltage value.

bias_current —— Displays the threshold of the DDM Bias Current value.

tx_power —— Displays the threshold of the DDM Tx Power value.

rx_power —— Displays the threshold of the DDM Rx Power value.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

View the DDM configuration state:

Device(config)#show ddm configuration state

View the threshold of the DDM Voltage value:

Device(config)#show ddm configuration voltage

19.9 show ddm status

Description

The **show ddm status** command is used to display the DDM status, which is the digital diagnostic monitoring status of SFP modules inserting into the device's SFP ports.

Syntax

show ddm status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

View the DDM status:

```
Device(config)#show ddm status
```

Chapter 20 Etherchannel Commands

Etherchannel Commands are used to configure LAG and LACP function.

LAG (Link Aggregation Group) is to combine a number of ports together to make a single high-bandwidth data path, which can highly extend the bandwidth. The bandwidth of the LAG is the sum of bandwidth of its member port.

LACP (Link Aggregation Control Protocol) is defined in IEEE802.3ad and enables the dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. The device can dynamically group similarly configured ports into a single logical link, which will highly extend the bandwidth and flexibly balance the load.

20.1 channel-group

Description

The **channel-group** command is used to add a port to the EtherChannel Group and configure its mode. To delete the port from the EtherChannel Group, please use **no channel-group** command.

Syntax

channel-group *num* **mode** { on | active | passive }

no channel-group

Parameter

num —— The number of the EtherChannel Group, ranging from 1 to 32.

on —— Enable the static LAG.

active —— Enable the active LACP mode.

passive —— Enable the passive LACP mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add ports 2-4 to EtherChannel Group 1 and enable the static LAG:

```
Device(config)# interface range gigabitEthernet 1/0/2-4
Device(config-if-range)# channel-group 1 mode on
```

20.2 port-channel load-balance

Description

The **port-channel load-balance** command is used to configure the Aggregate Arithmetic for LAG. To return to the default configurations, please use **no port-channel load-balance** command.

Syntax

port-channel load-balance { src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip }

no port-channel load-balance

Parameter

src-mac —— The source MAC address. When this option is selected, the Aggregate Arithmetic will be based on the source MAC address of the packets.

dst-mac —— The destination MAC address. When this option is selected, the Aggregate Arithmetic will be based on the destination MAC address of the packets.

src-dst-mac —— The source and destination MAC address. When this option is selected, the Aggregate Arithmetic will be based on the source and destination MAC addresses of the packets. The Aggregate Arithmetic for LAG is “src-dst-mac” by default.

src-ip —— The source IP address. When this option is selected, the Aggregate Arithmetic will be based on the source IP address of the packets.

dst-ip —— The destination IP address. When this option is selected, the Aggregate Arithmetic will be based on the destination IP address of the packets.

src-dst-ip —— The source and destination IP address. When this option is selected, the Aggregate Arithmetic will be based on the source and destination IP addresses of the packets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Aggregate Arithmetic for LAG as “src-dst-ip”:

Device(config)# port-channel load-balance src-dst-ip

20.3 lacp system-priority

Description

The **lacp system-priority** command is used to configure the LACP system priority globally. To return to the default configurations, please use **no lacp system-priority** command.

Syntax

lacp system-priority *pri*

no lacp system-priority

Parameter

pri—— The system priority, ranging from 0 to 65535. It is 32768 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the LACP system priority as 1024 globally:

Device(config)# lacp system-priority 1024

20.4 lacp port-priority

Description

The **lacp port-priority** command is used to configure the LACP port priority for specified ports. To return to the default configurations, please use **no lacp port-priority** command.

Syntax

lacp port-priority *pri*

no lacp port-priority

Parameter

pri—— The port priority, ranging from 0 to 65535. It is 32768 by default.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the LACP port priority as 1024 for ports 1-3:

Device(config)# interface range gigabitEthernet 1/0/1-3

Device(config-if-range)# lacp port-priority 1024

Configure the LACP port priority as 2048 for port 4:

Device(config)# interface gigabitEthernet 1/0/4

Device(config-if)# lacp port-priority 2048

20.5 show etherchannel

Description

The **show etherchannel** command is used to display the EtherChannel information.

Syntax

show etherchannel [*channel-group-num*] { detail | summary }

Parameter

channel-group-num —— The EtherChannel Group number, ranging from 1 to 14. By default, it is empty, and will display the information of all EtherChannel Groups.

detail —— The detailed information of EtherChannel.

summary —— The EtherChannel information in summary.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the detailed information of EtherChannel Group 1:

```
Device(config)# show etherchannel 1 detail
```

20.6 show etherchannel load-balance

Description

The **show etherchannel load-balance** command is used to display the Aggregate Arithmetic of LAG.

Syntax

show etherchannel load-balance

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Aggregate Arithmetic of LAG:

```
Device(config)# show etherchannel load-balance
```

20.7 show lacp

Description

The **show lacp** command is used to display the LACP information for a specified EtherChannel Group.

Syntax

show lacp [*channel-group-num*] { internal /neighbor }

Parameter

channel-group-num —— The EtherChannel Group number, ranging from 1 to 14. By default, it is empty, and will display the information of all LACP groups.

internal —— The internal LACP information.

neighbor —— The neighbor LACP information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the internal LACP information of EtherChannel Group 1:

```
Device(config)# show lacp 1 internal
```

20.8 show lacp sys-id

Description

The **show lacp sys-id** command is used to display the LACP system priority globally.

Syntax

show lacp sys-id

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LACP system priority:

```
Device(config)# show lacp sys-id
```

Chapter 21 MAC Address Commands

MAC Address configuration can improve the network security by configuring the Port Security and maintaining the address information by managing the Address Table.

21.1 mac address-table static

Description

The **mac address-table static** command is used to add the static MAC address entry. To remove the corresponding entry, please use **no mac address-table static** command. The static address can be added or removed manually, independent of the aging time. In the stable networks, the static MAC address entries can facilitate the device to reduce broadcast packets and enhance the efficiency of packets forwarding remarkably.

Syntax

mac address-table static *mac-addr* vid *vid* **interface** { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }

no mac address-table static *mac-addr* vid *vid* **interface** { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }

Parameter

mac-addr ——The MAC address of the entry you desire to add.

vid —— The VLAN ID number of your desired entry. It ranges from 1 to 4093.

port —— The Ethernet port number of your desired entry.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a static Mac address entry to bind the MAC address 00:02:58:4f:6c:23, VLAN1 and port 1 together:

Device(config)# mac address-table static 00:02:58:4f:6c:23 **vid** 1 **interface gigabitEthernet** 1/0/1

21.2 no mac address-table dynamic

Description

The **no mac address-table dynamic** command is used to delete the specified dynamic MAC address, or dynamic MAC addresses based on the VLAN or the port.

Syntax

no mac address-table dynamic { *mac-addr* | vid *vid* | interface {fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port*} }

Parameter

mac-addr ——The MAC address you desire to delete.

vid ——The VLAN ID on which you desire to delete MAC addresses.

port ——The Ethernet port on which you desire to delete MAC addresses.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete the MAC addresses on VLAN 1:

```
Device(config)# no mac address-table dynamic vid 1
```

21.3 mac address-table aging-time

Description

The **mac address-table aging-time** command is used to configure aging time for the dynamic address. To return to the default configuration, please use **no mac address-table aging-time** command.

Syntax

mac address-table aging-time *aging-time*

no mac address-table aging-time

Parameter

aging-time —— The aging time for the dynamic address. The value of it can be 0 or ranges from 10 to 630 seconds. When 0 is entered, the Auto Aging function is disabled. It is 300 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the aging time as 500 seconds:

Device(config)# mac address-table aging-time 500

21.4 mac address-table filtering

Description

The **mac address-table filtering** command is used to add the filtering address entry. To delete the corresponding entry, please use **no mac address-table filtering** command. The filtering address function is to forbid the undesired package to be forwarded. The filtering address can be added or removed manually, independent of the aging time.

Syntax

mac address-table filtering *mac-addr* **vid** *vid*

no mac address-table filtering {[*mac-addr*] [vid *vid*]}

Parameter

mac-addr —— The MAC address to be filtered.

vid —— The corresponding VLAN ID of the MAC address. It ranges from 1 to 4093.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a filtering address entry of which VLAN ID is 1 and MAC address is 00:1e:4b:04:01:5d:

Device(config)# mac address-table filtering 00:1e:4b:04:01:5d **vid** 1

21.5 mac address-table max-mac-count

Description

The **mac address-table max-mac-count** command is used to configure the Port Security. To return to the default configurations, please use **no mac address-table max-mac-count** command. Port Security is to protect the device from the malicious MAC address attack by limiting the maximum number of the MAC addresses that can be learned on the port. The port with Port Security feature enabled will learned the MAC address dynamically. When the learned MAC address number reaches the maximum, the port will stop learning. Therefore, the other devices with the MAC address unlearned cannot access to the network via this port.

Syntax

mac address-table max-mac-count { [max-number *num*] [mode { dynamic | static | permanent }] [status { forward | drop | disable }] [exceed-max-learned enable | disable] }

no mac address-table max-mac-count [max-number | mode | status]

Parameter

num —— The maximum number of MAC addresses that can be learned on the port. It ranges from 0 to 64. By default, this value is 64.

dynamic | static | permanent —— Learn mode for MAC addresses. There are three modes, including Dynamic mode, Static mode and Permanent mode. When Dynamic mode is selected, the learned MAC address will be deleted automatically after the aging time. When Static mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the device is rebooted. When permanent mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually too. However, the learned entries will be saved even the device is rebooted.

status —— Select the action to be taken when the number of the MAC addresses reaches the maximum learning number on the port. By default, this function is disabled.

- forward: The packets will be forward but not be learned when learned MAC number exceeds the maximum MAC address number on this port.
- drop: The packets will be dropped when learned MAC number exceeds the maximum MAC address number on this port.
- disable: The MAC address threshold on this port is disabled.

new-mac-learned enable | disable —— Enable/Disable the new-mac-learned notification on this port. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the port learns a new MAC address.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable Port Security function for port 1/0/1, select Static mode as the learn mode, and specify the maximum number of MAC addresses that can be learned on this port as 30. When the number of MAC address entries reaches 30 on this port, new entry will be dropped:

```
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# mac address-table max-mac-count max-number 30
mode static status drop
```

21.6 show mac address-table

Description

The **show mac address-table** command is used to display the information of all address entries.

Syntax

show mac address-table { dynamic | static | filtering }

Parameter

dynamic | static | filtering —— The type of your desired entry. By default, all the entries are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all address entries:

```
Device(config)# show mac address-table
```

21.7 clear mac address-table

Description

The **clear mac address-table** command is used to clear the specified address entries.

Syntax

clear mac address-table { dynamic | static | filtering }

Parameter

dynamic | static | filtering —— The type of your desired entry.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the information of all static address entries:

```
Device(config)# clear mac address-table static
```

21.8 show mac address-table aging-time

Description

The **show mac address-table aging-time** command is used to display the Aging Time of the MAC address.

Syntax

show mac address-table aging-time

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Aging Time of the MAC address:

```
Device(config)# show mac address-table aging-time
```

21.9 show mac address-table max-mac-count

Description

The **show mac address-table max-mac-count interface gigabitEthernet** command is used to display the security configuration of all ports or the specified port.

Syntax

show mac address-table max-mac-count { all | interface gigabitEthernet *port*}

Parameter

all —— Displays the security information of all the Ethernet ports.

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration of all ports:

```
Device(config)# show mac address-table max-mac-count all
```

Display the security configuration of port 1/0/1:

```
Device(config)# show mac address-table max-mac-count interface
gigabitEthernet 1/0/1
```

21.10 show mac address-table interface

Description

The **show mac address-table interface** command is used to display the address configuration of the specified port/port channel.

Syntax

show mac address-table interface { gigabitEthernet *port* | port-channel *port-channel-id*} | gpon *pon-port* [ont *ont-id*]}

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

pon-port—— The PON port list of the ONT.

ont-id—— The ID of the ONT.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the address configuration of port 1/0/1:

```
Device(config)# show mac address-table interface gigabitEthernet 1/0/1
```

21.11 show mac address-table count

Description

The **show mac address-table count** command is used to display the total amount of MAC address table.

Syntax

show mac address-table count [vlan *vlan-id*]

Parameter

vlan-id —— Specify the VLAN which the MAC entries belong to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the total MAC entry information in different VLANs:

```
Device(config)# show mac address-table count
```

21.12 show mac address-table address

Description

The **show mac address-table address** command is used to display the information of the specified MAC address.

Syntax

show mac address-table address *mac-addr* [interface { gigabitEthernet *port* | port-channel *port-channel-id*} | vid *vlan-id*]

Parameter

mac-addr——The specified MAC address.

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

vlan-id—— Specify the VLAN which the entry belongs to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the MAC address 00:00:00:00:23:00 in VLAN 1:

Device(config)#show mac address-table address 00:00:00:00:23:00 **vid** 1

21.13 show mac address-table vlan

Description

The **show mac address-table vlan** command is used to display the MAC address configuration of the specified vlan.

Syntax

show mac address-table vlan *vid*

Parameter

vid——The specified VLAN id.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MAC address configuration of vlan 1:

Device(config)# show mac address-table vlan 1

Chapter 22 IEEE 802.1Q VLAN Commands

VLAN (Virtual Local Area Network) technology is developed for the device to divide the LAN into multiple logical LANs flexibly. Hosts in the same VLAN can communicate with each other, regardless of their physical locations. VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

22.1 vlan

Description

The **vlan** command is used to create IEEE 802.1Q VLAN and enter VLAN Configuration Mode. To delete the IEEE 802.1Q VLAN, please use **no vlan** command.

Syntax

vlan *vlan-list*

no vlan *vlan-list*

Parameter

vlan-list —— Specify IEEE 802.1Q VLAN ID list, ranging from 1 to 4093, in the format of 2-3, 5. It is multi-optional.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VLAN 2-10 and VLAN 100:

```
Device(config)# vlan 2-10,100
```

Delete VLAN 2:

```
Device(config)# no vlan 2
```

22.2 interface vlan

Description

The **interface vlan** command is used to create VLAN Interface hereafter to

access to Interface VLAN Mode.

Syntax

interface vlan *vlan-id*

no interface vlan *vlan-id*

Parameter

vlan-id——Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4093.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VLAN Interface 2:

```
Device(config)# interface vlan 2
```

22.3 name

Description

The **name** command is used to assign a description to a VLAN. To clear the description, please use **no name** command.

Syntax

name *descript*

no name

Parameter

descript——String to describe the VLAN, which contains 16 characters at most.

Command Mode

VLAN Configuration Mode(VLAN)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the name of VLAN 2 as “group1”:

Device(config)# vlan 2

Device(config-vlan)# name group1

22.4 switchport general allowed vlan

Description

The **switchport general allowed vlan** command is used to add the desired port to IEEE 802.1Q VLAN, or to remove a port from the corresponding VLAN.

Syntax

switchport general allowed vlan *vlan-list* { tagged | untagged }

no switchport general allowed vlan *vlan-list*

Parameter

vlan-list —— VLAN ID list, ranging from 1 to 4093, in the format of 2-3, 5. It is multi-optional.

tagged | untagged —— egress-rule.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure Gigabit Ethernet port 1/0/4 whose link type is "general" to VLAN 2 and its egress-rule as "tagged":

Device(config)#interface gigabitEthernet 1/0/4

Device(config-if)#switchport general allowed vlan 2 tagged

22.5 switchport pvid

Description

The **switchport pvid** command is used to configure the PVID for the switch ports.

Syntax

switchport pvid *vlan-id*

Parameter

vlan-id—— VLAN ID, ranging from 1 to 4093.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the PVID of port 1/0/2 as 2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# switchport pvid 2

22.6 switchport check ingress

Description

The **switchport check ingress** command is used to enable the Ingress Checking function for the switch ports. With this function enabled, the port will accept the packet of which the VLAN ID is in the port's VLAN list and discard others. With this function disabled, the port will forward the packet directly. To disable this function, please use **no switchport check ingress** command.

Syntax

switchport check ingress

no switchport check ingress

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable Ingress Checking on the port 1/0/2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# switchport check ingress

22.7 switchport acceptable frame

Description

The **switchport acceptable frame** command is used to specify the acceptable frame type for the switch ports and the ports will perform this operation before Ingress Checking. To restore to the default setting, please use **no switchport acceptable frame** command.

Syntax

switchport acceptable frame { all | tagged }

no switchport acceptable frame

Parameter

all | tagged —— the acceptable frame type.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the acceptable frame type of Gigabit Ethernet port 1/0/4 as “tagged”:

Device(config)#interface gigabitEthernet 1/0/4

Device(config-if)#switchport acceptable frame general

22.8 show vlan summary

Description

The **show vlan summary** command is used to display the summarized information of IEEE 802.1Q VLAN.

Syntax

show vlan summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summarized information of IEEE 802.1Q VLAN:

```
Device(config)# show vlan summary
```

22.9 show vlan brief

Description

The **show vlan brief** command is used to display the brief information of IEEE 802.1Q VLAN.

Syntax

show vlan brief

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the brief information of IEEE 802.1Q VLAN:

```
Device(config)# show vlan brief
```

22.10 show vlan

Description

The **show vlan** command is used to display the information of IEEE 802.1Q VLAN.

Syntax

show vlan [id *vlan-id*]

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094. It is multi-optional. Using the **show vlan** command without parameter displays the detailed information of all VLANs.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of vlan 5:

```
Device(config)# show vlan id 5
```

22.11 show interface switchport

Description

The **show interface switchport** command is used to display the IEEE 802.1Q VLAN configuration information of the specified port/port channel.

Syntax

show interface switchport [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the VLAN configuration information of all ports and port channels:

```
Device(config)# show interface switchport
```

Chapter 23 MAC-based VLAN Commands

MAC VLAN (Virtual Local Area Network) is the way to classify the VLANs based on MAC Address. A MAC address is relative to a single VLAN ID. The untagged packets and the priority-tagged packets coming from the MAC address will be tagged with this VLAN ID.

23.1 mac-vlan mac-address

Description

The **mac-vlan mac-address** command is used to create a MAC-based VLAN entry. To delete a MAC-based VLAN entry, please use the **no mac-vlan mac-address** command.

Syntax

mac-vlan mac-address *mac-addr* **vlan** *vlan-id* [description *descript*]

no mac-vlan mac-address *mac-addr*

Parameter

mac-addr —— MAC address, in the format of XX:XX:XX:XX:XX:XX.

vlan-id —— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4093.

descript —— Give a description to the MAC address for identification, which contains 8 characters at most.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create VLAN 2 with the MAC address 00:11:11:01:01:12 and the name “TP”:

Device(config)#mac-vlan mac-address 00:11:11:01:01:12 **vlan** 2

description TP

23.2 mac-vlan

Description

The **mac-vlan** command is used to enable a port for the MAC-based VLAN feature. Only the port is enabled can the configured MAC-based VLAN take effect. To disable the MAC-based VLAN function, please use **no mac-vlan** command. All the ports are disabled by default.

Syntax

mac-vlan

no mac-vlan

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Gigabit Ethernet port 1/0/3 for the MAC-based VLAN feature:

Device(config)#interface gigabitEthernet 1/0/3

Device(config-if)#mac-vlan

23.3 show mac-vlan

Description

The **show mac-vlan** command is used to display the information of the MAC-based VLAN entry. MAC address and VLAN ID can be used to filter the displayed information.

Syntax

show mac-vlan { all | mac-address *mac-addr* | vlan *vlan-id*}

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Parameter

mac-addr —— MAC address, in the format of XX:XX:XX:XX:XX:XX.

vlan-id —— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

Example

Display the information of all the MAC-based VLAN entry:

```
Device(config)#show mac-vlan all
```

23.4 show mac-vlan interface

Description

The **show mac-vlan interface** command is used to display the port state of MAC-based VLAN.

Syntax

show mac-vlan interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the enable state of all the ports:

```
Device(config)#show mac-vlan interface
```

Chapter 24 Protocol-based VLAN Commands

Protocol VLAN (Virtual Local Area Network) is the way to classify VLANs based on Protocols. A Protocol is relative to a single VLAN ID. The untagged packets and the priority-tagged packets matching the protocol template will be tagged with this VLAN ID.

24.1 protocol-vlan template

Description

The **protocol-vlan template** command is used to create Protocol-based VLAN template. To delete Protocol-based VLAN template, please use **no protocol-vlan template** command.

Syntax

protocol-vlan template name *protocol-name* **frame** { ether_2 ether-type *type* | snap ether-type *type* | llc dsap *dsap_type* ssap *ssap_type* }

no protocol-vlan template *template-idx*

Parameter

protocol-name —— Give a name for the Protocol-based VLAN Template , which contains 8 characters at most.

ether_2 ether-type *type* —— Specify the Ethernet type.

snap ether-type *type* —— Specify the Ethernet type.

llc dsap *dsap_type* **ssap** *ssap_type* —— Specify the DSAP type and the SSAP type.

template-idx —— The number of the Protocol-based VLAN Template. You can get the template corresponding to the number by the show protocol-vlan template command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a Protocol-based VLAN template named “TP” whose Ethernet protocol type is 0x2024:

Device(config)#protocol-vlan template name TP **frame ether_2 ether-type** 2024

24.2 protocol-vlan vlan

Description

The **protocol-vlan vlan** command is used to create a Protocol-based VLAN entry. To delete a Protocol-based VLAN entry, please use **no protocol-vlan vlan** command.

Syntax

protocol-vlan vlan *vlan-id* **priority** *priority* **template** *template-idx*

no protocol-vlan vlan *group-idx*

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1-4093.

priority—— Specify the 802.1p priority for the packets that belong to the protocol VLAN, ranging from 0–7. The device will determine the forwarding sequence according this value. The packets with larger value of 802.1p priority have the higher priority.

template-idx——The number of the Protocol-based VLAN Template. You can get the template corresponding to the number by the show protocol-vlan template command.

group-idx——The number of the Protocol-based VLAN entry. You can get the Protocol-based VLAN entry corresponding to the number by the show protocol-vlan vlan command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create Protocol-based VLAN 2 and bind it with Protocol-based VLAN Template 3:

```
Device(config)#protocol-vlan vlan 2 template 3
```

24.3 protocol-vlan group

Description

The **protocol-vlan** command is used to add the port to a specified protocol group. To remove the port from this protocol group, please use **no protocol-vlan group** command.

Syntax

protocol-vlan group *index*

no protocol-vlan group *index*

Parameter

index—— Specify the protocol group ID.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add Gigabit Ethernet port 20 to protocol group 1:

```
Device(config)#interface gigabitEthernet 1/0/20
Device(config-if)#protocol-vlan group 1
```

24.4 show protocol-vlan template

Description

The **show protocol-vlan template** command is used to display the information of the Protocol-based VLAN templates.

Syntax

show protocol-vlan template

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the Protocol-based VLAN templates:

```
Device(config)#show protocol-vlan template
```

24.5 show protocol-vlan vlan

Description

The **show protocol-vlan vlan** command is used to display the information about Protocol-based VLAN entry.

Syntax

show protocol-vlan vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display information of the Protocol-based VLAN entry:

```
Device(config)#show protocol-vlan vlan
```

Chapter 25 GVRP Commands

GVRP (GARP VLAN registration protocol) is an implementation of GARP (generic attribute registration protocol). GVRP allows the device to automatically add or remove the VLANs via the dynamic VLAN registration information and propagate the local VLAN registration information to other devicees, without having to individually configure each VLAN.

25.1 gvrp

Description

The **gvrp** command is used to enable the GVRP function globally. To disable the GVRP function, please use **no gvrp** command.

Syntax

gvrp

no gvrp

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the GVRP function globally:

```
Device(config)#gvrp
```

25.2 gvrp (interface)

Description

The **gvrp** command is used to enable the GVRP function for the desired port. To disable it, please use **no gvrp** command. The GVRP feature can only be enabled for the trunk-type ports.

Syntax

gvrp

no gvrp

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the GVRP function for Gigabit Ethernet ports 1/0/2-6:

```
Device(config)#interface range gigabitEthernet 1/0/2-6
Device(config-if-range)#gvrp
```

25.3 gvrp registration

Description

The **gvrp registration** command is used to configure the GVRP registration type for the desired port. To restore to the default value, please use **no gvrp registration** command.

Syntax

gvrp registration { normal | fixed | forbidden }

no gvrp registration

Parameter

normal | fixed | forbidden —— Registration mode. By default, the registration mode is “normal”.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the GVRP registration mode as "fixed" for Gigabit Ethernet ports 1/0/2-6:

Device(config)#interface range gigabitEthernet 1/0/2-6

Device(config-if-range)#gvrp registration fixed

25.4 gvrp timer

Description

The **gvrp timer** command is used to set a GVRP timer for the desired port. To restore to the default setting of a GARP timer, please use **no gvrp timer** command.

Syntax

gvrp timer { leaveall | join | leave } *value*

no gvrp timer [leaveall | join | leave]

Parameter

leaveall | join | leave —— They are the three timers: leave All, join and leave. Once the LeaveAll Timer is set, the port with GVRP enabled can send a LeaveAll message after the timer times out, so that other GARP ports can re-register all the attribute information. After that, the LeaveAll timer will start to begin a new cycle. To guarantee the transmission of the Join messages, a GARP port sends each Join message two times. The Join Timer is used to define the interval between the two sending operations of each Join message. Once the Leave Timer is set, the GARP port receiving a Leave message will start its Leave timer, and deregister the attribute information if it does not receive a Join message again before the timer times out.

value ——The value of the timer. The LeaveAll Timer ranges from 1000 to 30000 centiseconds and the default value is 1000 centiseconds. The Join Timer ranges from 20 to 1000 centiseconds and the default value is 20 centiseconds. The Leave Timer ranges from 60 to 3000 centiseconds and the default value is 60 centiseconds.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the GARP leaveall timer of Gigabit Ethernet port 1/0/6 as 2000 centiseconds and restore the join timer of it to the default value:

```
Device(config)#interface gigabitEthernet 1/0/6
Device(config-if)#gvrp timer leaveall 2000
Device(config-if)#no gvrp timer join
```

25.5 show gvrp interface

Description

The **show gvrp interface** command is used to display the GVRP configuration information of a specified Ethernet port or of all Ethernet ports.

Syntax

show gvrp interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port —— The port number.
port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the GVRP configuration information of Gigabit Ethernet port 1:

```
Device(config)#show gvrp interface gigabitEthernet 1/0/1
```

Display the GVRP configuration information of all Ethernet ports:

```
Device(config)#show gvrp interface
```

25.6 show gvrp global

Description

The **show gvrp global** command is used to display the global GVRP status.

Syntax

show gvrp global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global GVRP status:

```
Device(config)#show gvrp global
```

Chapter 26 IGMP Snooping Commands

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on Layer 2 device. It can effectively prevent multicast groups being broadcasted in the network.

26.1 ip igmp snooping (global)

Description

The **ip igmp snooping** command is used to configure IGMP Snooping globally. To disable the IGMP Snooping function, please use **no ip igmp snooping** command.

Syntax

ip igmp snooping

no ip igmp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP Snooping function:

```
Device(config)# ip igmp snooping
```

26.2 ip igmp snooping version

Description

The **ip igmp snooping version** command is used to configure IGMP version globally. To return to the default configuration, please use **no ip igmp snooping version** command.

Syntax

ip igmp snooping version {v1 | v2 | v3 }

no ip igmp snooping version

Parameter

v1 | v2 | v3—— Specify the IGMP version. By default, it is IGMP v3.

v1: The device works as an IGMPv1 Snooping device. It can only process IGMPv1 messages from the host. Report messages of other versions are ignored.

v2: The device works as an IGMPv2 Snooping device. It can process both IGMPv1 and IGMPv2 messages from the host. IGMPv3 messages are ignored.

v3: The device works as an IGMPv3 Snooping device. It can process IGMPv1, IGMPv2 and IGMPv3 messages from the host.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the IGMP version as v2:

```
Device (config)# ip igmp snooping version v2
```

26.3 ip igmp snooping drop-unknown

Description

The **ip igmp snooping drop-unknown** command is used to configure the way how the device processes multicast streams that are sent to unknown multicast groups as Discard. By default, it is Forward. To return to the default configuration, please use **no ip igmp snooping drop-unknown** command.

Syntax

ip igmp snooping drop-unknown

no ip igmp snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the operation to process unknown multicast as discard:

```
Device(config)# ip igmp snooping drop-unknown
```

26.4 ip igmp snooping header-validation

Description

The **ip igmp snooping header-validation** command is used to enable IGMP Header Validation globally. To disable the IGMP Header Validation function, please use **no ip igmp snooping header-validation** command.

Generally, for IGMP packets, the TTL value should be 1, ToS field should be 0xC0, and Router Alert option should be 0x94040000. The fields to be validated depend on the IGMP version being used. IGMPv1 only checks the TTL field. IGMPv2 checks the TTL field and the Router Alert option. IGMPv3 checks TTL field, ToS field and Router Alert option. Packets that fail the validation process will be dropped.

Syntax

ip igmp snooping header-validation

no ip igmp snooping header-validation

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP Header Validation:

```
Device(config)# ip igmp snooping header-validation
```

26.5 ip igmp snooping vlan-config

Description

The **ip igmp snooping vlan-config** command is used to enable VLAN IGMP Snooping function or to modify IGMP Snooping parameters. To disable the VLAN IGMP Snooping function, please use **no ip igmp snooping vlan-config** command. To restore the default values, please use **no ip igmp snooping vlan-config** with specified parameters.

Syntax

ip igmp snooping vlan-config *vlan-id-list* [rtime *router-time* | mtime *member-time* | ltime *leave-time*]

no ip igmp snooping vlan-config *vlan-id-list* [rtime | mtime | ltime]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

router-time —— The Router Port Aging Time. Within this time, if the device does not receive IGMP query message from the router port, it will consider this port is not a router port any more. Valid values are from 60 to 600 in seconds, and the default value is 300 seconds.

member-time —— The Member Port Aging Time. Within this time, if the device does not receive IGMP report message from the member port, it will consider this port is not a member port any more. Valid values are from 60 to 600 in seconds, and the default value is 260 seconds.

leave-time —— The Leave Time. Valid values are from 1 to 30 in seconds, and the default value is 1 second. When the device receives a leave message from a port to leave a multicast group, it will wait for a Leave Time before removing the port from the multicast group. During the period, if the device receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

- If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends.
- The Leave Time mechanism will not take effect when Fast Leave takes effect.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IGMP Snooping function and modify Router Port Aging Time as 300 seconds, Member Port Aging Time as 200 seconds for VLAN 1-3:

Device(config)# ip igmp snooping vlan-config 1-3 **rtime** 300

Device(config)# ip igmp snooping vlan-config 1-3 **mtime** 200

26.6 ip igmp snooping vlan-config (immediate-leave)

Description

This command is used to enable the Fast Leave feature for specific VLANs. To disable Fast Leave on the VLANs, please use **no ip igmp snooping vlan-config** *vlan-id-list* **immediate-leave** command. This function is disabled by default.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **immediate-leave**

no ip igmp snooping vlan-config *vlan-id-list* **immediate-leave**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Fast Leave for VLAN 1-3:

```
Device(config)# ip igmp snooping vlan-config 1-3 immediate-leave
```

26.7 ip igmp snooping vlan-config (report-suppression)

Description

This command is used to enable the IGMP Report Suppression function for specific VLANs. When enabled, the device will only forward the first IGMP report message for each multicast group to the IGMP querier and suppress subsequent IGMP report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the IGMP querier. To disable the IGMP report suppression function and forward all the IGMP reports to the Layer 3 device in specific VLANs,

please use **no ip igmp snooping vlan-config** *vlan-id-list* **report-suppression** command. This function is disabled by default.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **report-suppression**

no ip igmp snooping vlan-config *vlan-id-list* **report-suppression**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IGMP Report Suppression for VLAN 1-3:

Device(config)# ip igmp snooping vlan-config 1-3 **report-suppression**

26.8 ip igmp snooping vlan-config (router-ports-forbidden)

Description

This command is used to forbid the specified ports as being router ports in the specified VLAN(s). To delete the forbidden router ports, please use **no ip igmp snooping vlan-config** *vlan-id-list* **router-ports-forbidd** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** { gigabitEthernet *port-list* | port-channel *port-channel-list* }

no ip igmp snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** [gigabitEthernet *port-list* | port-channel *port-channel-list*]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— Forbid the specified ports as being router ports. Packets sent from multicast routers to these ports will be discarded.

port-channel-list —— Forbid the specified port-channels as being router ports. Packets sent from multicast routers to these port-channels will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Forbid the Ethernet ports 1/0/1-3 as being router ports in VLAN 1 :

Device(config)# ip igmp snooping vlan-config 1 **router-ports-forbidd interface gigabitEthernet** 1/0/1-3

26.9 ip igmp snooping vlan-config (rport interface)

Description

This command is used to specify the static router ports for specific VLANs. To delete the static router ports, please use **no ip igmp snooping vlan-config** *vlan-id-list* **rport interface** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **rport interface** { gigabitEthernet *port-list* | port-channel *port-channel-list* }

no ip igmp snooping vlan-config *vlan-id-list* **rport interface** { gigabitEthernet *port-list* | port-channel *port-channel-list* }

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— The list of Ethernet ports.

port-channel-list—— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the router port as 1/0/1 for VLAN 1-2:

Device(config)# ip igmp snooping vlan-config 1-2 **rport interface gigabitEthernet** 1/0/1

26.10 ip igmp snooping vlan-config (static)

Description

This command is used to configure interfaces to statically join a multicast group. To remove interfaces from a static multicast group, please use **no ip igmp snooping vlan-config** *vlan-id-list* **static**command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **static** *ip* **interface** { gpon *port-list*}

no ip igmp snooping vlan-config *vlan-id-list* **static** *ip* **interface** { gpon *port-list*}

Parameter

vlan-id-list—— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

ip——Specify the IP address of the multicast group that the hosts want to join.

port-list—— The list of Ethernet ports.

port-channel-list—— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure port ports 1/0/1-3 in VLAN 2 to statically join multicast group 225.0.0.1:

Device(config)# ip igmp snooping vlan-config 2 **static** 225.0.0.1 **interface gigabitEthernet** 1/0/1-3

26.11 ip igmp snooping vlan-config (querier)

Description

This command is used to enable the IGMP Snooping Querier feature for specific VLANs. To disable the IGMP Snooping Querier feature on the VLANs, please use **no ip igmp snooping vlan-config** *vlan-id-list* **querier** command without any parameters. To restore the default values, please use **no ip igmp snooping vlan-config** *vlan-id-list* **querier** command with specified parameters.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **querier** [max-response-time *response-time* | query-interval *interval* | general-query source-ip *ip-addr* | last-member-query-count *count* | last-member-query-interval *interval*]

no ip igmp snooping vlan-config *vlan-id-list* **querier** [max-response-time | query-interval | general-query source-ip | last-member-query-count]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

response-time—— The host's maximum response time to general query messages. Valid values are from 1 to 25 seconds, and the default value is 10 seconds.

query-interval *interval*—— The interval between general query messages sent by the device. Valid values are from 10 to 300 seconds, and the default value is 60 seconds.

ip-addr—— The source IP address of the general query messages sent by the device. It should be a unicast address. By default, it is 0.0.0.0.

count —— The number of group-specific queries to be sent. With IGMP Snooping Querier enabled, when the device receives an IGMP leave message, it obtains the address of the multicast group that the host wants to leave from the message. Then the device sends out group-specific queries to this multicast group through the port receiving the leave message. If specified count of group-specific queries are sent and no report message is received, the device will delete the multicast address from the multicast forwarding table. Valid values are from 1 to 5, and the default value is 2.

last-member-query-interval *interval* —— The interval between group-specific queries.. Valid values are from 1 to 5 seconds, and the default value is 1 second.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IGMP Snooping Querier for VLAN 3, and configure the query interval as 100 seconds:

Device(config)# ip igmp snooping vlan-config 3 **querier**

Device(config)# ip igmp snooping vlan-config 3 **querier query interval** 100

26.12 ip igmp snooping (interface)

Description

The **ip igmp snooping** command is used to enable the IGMP Snooping function for the desired port. To disable the IGMP Snooping function, please use **no ip igmp snooping** command.

Syntax

ip igmp snooping

no ip igmp snooping

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IGMP Snooping function of port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# ip igmp snooping

26.13 ip igmp snooping max-groups

Description

The **ip igmp snooping max-groups** command is used to configure the maximum number of groups that a port can join in. The **ip igmp snooping max-groups action** is used to configure the action that the port takes when it receives an IGMP report message and the maximum number of entries is in the forwarding table. To remove the maximum group limitation and return to the default of no limitation on the specified port, please use the **no ip igmp snooping max-groups** command. To return to the default action of dropping the report, please use the **no ip igmp snooping max-groups action** command. These commands only apply to the dynamic multicast groups.

Syntax

ip igmp snooping max-groups *maxgroup*

ip igmp snooping max-groups action { drop | replace }

no ip igmp snooping max-groups

no ip igmp snooping max-groups action

Parameter

maxgroup —— Specify the maximum numbers of groups that the port can join. It ranges from 0 to 1000 and the default value is 1000.

drop —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the port will not join any new multicast group.

replace —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the maximum numbers of groups that ports 1/0/2-5 can join as 10, and configure the throttling action as replace:

Device(config)#interface range gigabitEthernet 1/0/2-5

Device(config-if-range)#ip igmp snooping max-groups 10

Device(config-if-range)#ip igmp snooping max-groups action replace

26.14 ip igmp snooping immediate-leave

Description

The **ip igmp snooping immediate-leave** command is used to configure the Fast Leave function for port. To disable the Fast Leave function, please use **no ip igmp snooping immediate-leave** command.

Syntax

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Fast Leave function for port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# ip igmp snooping immediate-leave

26.15 ip igmp profile

Description

The **ip igmp profile** command is used to create the configuration profile. To delete the corresponding profile, please use **no ip igmp profile** command.

Syntax

ip igmp profile *id*

no ip igmp profile *id*

Parameter

id—— Specify the id of the configuration profile, ranging from 1 to 999.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the profile 1:

Device(config)# ip igmp profile 1

26.16 deny

Description

The **deny** command is used to configure the filtering mode of profile as deny.

Syntax

deny

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the filtering mode of profile 1 as deny:

Device(config)# ip igmp profile 1

Device(config-igmp-profile)#deny

26.17 permit

Description

The **permit** command is used to configure the filtering mode of profile as permit.

Syntax

permit

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the filtering mode of profile 1 as permit:

```
Device(config)# ip igmp profile 1
Device(config-igmp-profile)#permit
```

26.18 range

Description

The **range** command is used to configure the range of the profile's filtering multicast address. To delete the corresponding filtering multicast address, please use **no range** command. A profile contains 16 filtering IP-range entries at most.

Syntax

range *start-ip end-ip*

no range *start-ip end-ip*

Parameter

start-ip —— The start filtering multicast IP address.

end-ip —— The end filtering multicast IP address.

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure one of the filter multicast address entry as range 225.1.1.1 to 226.3.2.1 in profile 1:

Device(config)# ip igmp profile 1

Device(config-igmp-profile)#range 225.1.1.1 226.3.2.1

26.19 ip igmp filter

Description

The **ip igmp filter** command is used to bind the specified profile to the interface. To delete the binding, please use **no ip igmp filter** command.

Syntax

ip igmp filter *profile-id*

no ip igmp filter

Parameter

profile-id—— Specify the profile ID, ranging from 1 to 999.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind profile 1 to interface gigabitEthernet 1/0/2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# ip igmp filter 1

26.20 clear ip igmp snooping statistics

Description

The **clear ip igmp snooping statistics** command is used to clear the statistics of the IGMP packets.

Syntax

clear ip igmp snooping statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the statistics of the IGMP packets:

```
Device(config)# clear ip igmp snooping statistics
```

26.21 show ip igmp snooping

Description

The **show ip igmp snooping** command is used to display the global configuration of IGMP snooping.

Syntax

show ip igmp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of IGMP:

```
Device# show ip igmp snooping
```

26.22 show ip igmp snooping interface

Description

The **show ip igmp snooping interface** command is used to display the port configuration of IGMP snooping. If no interface is specified, it displays all interfaces' IGMP snooping configurations.

Syntax

show ip igmp snooping interface [gigabitEthernet [*port-list*] | port-channel [*port-channel-list*]] {authentication | basic-config | max-groups | packet-stat}

Parameter

port-list —— The list of Ethernet ports.

Port-channel-list —— The list of port channels.

authentication | basic-config | max-groups | packet-stat —— The related configuration information selected to display.

Note: Authentication is only available on certain devices.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP baisic configuration configuration of all ports and port channels:

Device# show ip igmp snooping interface basic-config

Display the IGMP basic configuration of port 1/0/2:

Device# show ip igmp snooping interface gigabitEthernet 1/0/2 basic-config

Display the IGMP packet statistics of ports 1/0/1-4:

Device# show ip igmp snooping interface gigabitEthernet 1/0/1-4 packet-stat

26.23 show ip igmp snooping vlan

Description

The **show ip igmp snooping vlan** command is used to display the VLAN configuration of IGMP snooping.

Syntax

show ip igmp snooping vlan [*vlan-id*]

Parameter

vlan-id——The VLAN ID selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP snooping configuration information of VLAN 2:

```
Device# show ip igmp snooping vlan 2
```

26.24 show ip igmp snooping groups

Description

The **show ip igmp snooping groups** command is used to display the information of all IGMP snooping groups. It can be extended to some other commands to display the dynamic and static multicast information of a selected VLAN.

Syntax

show ip igmp snooping groups [vlan {*vlan-id*}] [*multicast_addr* | count | dynamic | dynamic count | static | static count]

Parameter

vlan-id——The VLAN ID selected to display the information of all multicast items.

multicast_addr—— IP address of the multicast group.

count—— The numbers of all multicast groups.

dynamic—— Display dynamic multicast groups.

dynamic count—— The numbers of all dynamic multicast groups.

static—— Display static multicast groups.

static count—— The numbers of all static multicast groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all IGMP snooping groups:

```
Device#show ip igmp snooping groups
```

Display all the multicast entries in VLAN 5:

```
Device(config)#show ip igmp snooping groups vlan 5
```

Display the count of multicast entries in VLAN 5:

```
Device(config)#show ip igmp snooping groups vlan 5 count
```

Display the dynamic multicast groups of VLAN 5

Device(config)#show ip igmp snooping groups vlan 5 dynamic

Display the static multicast groups of VLAN 5

Device(config)#show ip igmp snooping groups vlan 5 static

Display the count of dynamic multicast entries of VLAN 5

Device(config)#show ip igmp snooping groups vlan 5 dynamic count

Display the count of static multicast entries of VLAN 5

Device(config)#show ip igmp snooping groups vlan 5 static count

26.25 show ip igmp profile

Description

The **show ip igmp profile** command is used to display the configuration information of all the profiles or a specific profile.

Syntax

show ip igmp profile [*id*]

Parameter

id —— Specify the ID of the profile, ranging from 1 to 999.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of all profiles:

Device(config)# show ip igmp profile

Chapter 27 MLD Snooping Commands

MLD Snooping (Multicast Listener Discovery Snooping) is a multicast control mechanism running on Layer 2 device. It can effectively prevent multicast groups being broadcasted in the IPv6 network.

27.1 ipv6 mld snooping (global)

Description

The **ipv6 mld snooping** command is used to enable MLD Snooping function globally. If this function is disabled, all related MLD Snooping function would not work. To disable this function, please use **no ipv6 mld snooping** command.

Syntax

ipv6 mld snooping

no ipv6 mld snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable MLD Snooping:

```
Device(config)# ipv6 mld snooping
```

27.2 ipv6 mld snooping drop-unknown

Description

The **ipv6 mld snooping drop-unknown** command is used to enable the unknown multicast packets filter function. To disable this function, please use **no ipv6 mld snooping drop-unknown** command. By default, it is disabled.

Syntax

ipv6 mld snooping drop-unknown

no ipv6 mld snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable unknown multicast filter function:

```
Device(config)# ipv6 mld snooping drop-unknown
```

27.3 ipv6 mld snooping vlan-config

Description

The **ipv6 mld snooping vlan-config** command is used to enable VLAN MLD Snooping function or to modify MLD Snooping parameters. To disable the VLAN MLD Snooping function, please use **no ipv6 mld snooping vlan-config** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* [rtime *router-time* | mtime *member-time* | ltime *leave-time*]

no ipv6 mld snooping vlan-config *vlan-id-list* [rtime | mtime | ltime]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

router-time —— The Router Port Aging Time. Within this time, if the device does not receive any MLD query messages from the router port, it will consider this port is not a router port any more. Valid values are from 60 to 600 in seconds, and the default value is 300 seconds.

member-time —— The Member Port Aging Time. Within this time, if the device does not receive any MLD report messages from the member port, it will consider this port is not a member port any more. Valid values are from 60 to 600 in seconds, and the default value is 260 seconds.

leave-time —— The Leave Time. Valid values are from 1 to 30 in seconds, and the default value is 1 second. When the device receives a done message from a port to leave a multicast group, it will wait for a Leave Time before removing the port from the multicast group. During the period, if the device receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

- If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends.

- The Leave Time mechanism will not take effect when Fast Leave takes effect.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the MLD Snooping function and modify Router Port Time as 300 seconds, Member Port Time as 200 seconds for VLAN 1-3:

```
Device(config)# ipv6 mld snooping vlan-config 1-3 rtime 300
Device(config)# ipv6 mld snooping vlan-config 1-3 mtime 200
```

27.4 ipv6 mld snooping vlan-config (immediate-leave)

Description

This command is used to enable the Fast Leave feature for specific VLANs. To disable Fast Leave on the VLANs, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **immediate-leave** command. This function is disabled by default.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **immediate-leave**

no ipv6 mld snooping vlan-config *vlan-id-list* **immediate-leave**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Fast Leave for VLAN 1-3:

```
Device(config)# ipv6 mld snooping vlan-config 1-3 immediate-leave
```

27.5 ipv6 mld snooping vlan-config (report-suppression)

Description

This command is used to enable the MLD Report Suppression function for specific VLANs. When enabled, the device will only forward the first MLD report message for each multicast group to the MLD querier and suppress subsequent MLD report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the MLD querier. To disable the MLD report suppression function and forward all the MLD reports to the Layer 3 device in specific VLANs, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **report-suppression** command. This function is disabled by default.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **report-suppression**

no ipv6 mld snooping vlan-config *vlan-id-list* **report-suppression**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MLD Report Suppression for VLAN 1-3:

```
Device(config)# ipv6 mld snooping vlan-config 1-3 report-suppression
```

27.6 ipv6 mld snooping vlan-config (router-ports-forbidden)

Description

This command is used to forbid the specified ports as being router ports in the specified VLAN(s). To delete the forbidden router ports, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **router-ports-forbidd** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** { gigabitEthernet *port-list* | port-channel *port-channel-list* }

no ipv6 mld snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** [gigabitEthernet *port-list* | port-channel *port-channel-list*]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— Forbid the specified ports as being router ports. Packets sent from multicast routers to these ports will be discarded.

port-channel-list —— Forbid the specified port-channels as being router ports. Packets sent from multicast routers to these port-channels will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Forbid the Ethernet ports 1/0/1-3 as being router ports in VLAN 1:

```
Device(config)# ipv6 mld snooping vlan-config 1 router-ports-forbidd
interface gigabitEthernet 1/0/1-3
```

27.7 ipv6 mld snooping vlan-config (rport interface)

Description

This command is used to specify the static router ports for specific VLANs. To delete the static router ports, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **rport interface** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **rport interface** { gigabitEthernet *port-list* | port-channel *port-channel-list* }

no ipv6 mld snooping vlan-config *vlan-id-list* **rport interface** { gigabitEthernet *port-list* | port-channel *port-channel-list* }

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— The list of Ethernet ports.

port-channel-list—— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the router port as 1/0/1 for VLAN 1-2:

```
Device(config)# ipv6 mld snooping vlan-config 1-2 rport interface
gigabitEthernet 1/0/1
```

27.8 ipv6 mld snooping vlan-config (static)

Description

This command is used to configure interfaces to statically join a multicast group. To remove interfaces from a static multicast group, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **static**command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **static** *ip* **interface** { gpon *port-list*}

no ipv6 mld snooping vlan-config *vlan-id-list* **static** *ip* **interface** { gpon *port-list*}

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

ip ——Specify the IP address of the multicast group that the hosts want to join.

port-list —— The list of Ethernet ports.

port-channel-list —— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure port ports 1/0/1-3 in VLAN 2 to statically join multicast group ff80::1234:1:

Device(config)# ipv6 mld snooping vlan-config 2 **static** ff80::1234:1 **interface gigabitEthernet** 1/0/1-3

27.9 ipv6 mld snooping vlan-config (querier)

Description

This command is used to enable the MLD Snooping Querier feature for specific VLANs. To disable the MLD Snooping Querier feature on the VLANs, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **querier** command without any parameters. To restore the default values, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **querier** command with specified parameters.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **querier** [max-response-time *response-time* | query-interval *interval* | general-query source-ip *ip-addr* | last-listener-query-count *count* | last-listener-query-interval *interval*]

no ipv6 mld snooping vlan-config *vlan-id-list* **querier** [max-response-time | query-interval | general-query source-ip | last-listener-query-count | last-listener-query-interval]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

response-time—— The host's maximum response time to general query messages. Valid values are from 1 to 25 seconds, and the default value is 10 seconds.

query-interval *interval*—— The interval between general query messages sent by the device. Valid values are from 10 to 300 seconds, and the default value is 60 seconds.

ip-addr—— The source IP address of the general query messages sent by the device. It should be a unicast address. By default, it is fe80::2ff:ffff:fe00:1.

count —— The number of group-specific queries to be sent. With MLD Snooping Querier enabled, when the device receives an MLD done message, it obtains the address of the multicast group that the host wants to leave from the message. Then the device sends out group-specific queries to this multicast group through the port receiving the done message. If specified count of group-specific queries are sent and no report message is received, the device will delete the multicast address from the multicast forwarding table. Valid values are from 1 to 5, and the default value is 2.

last-member-query-interval *interval*—— The interval between group-specific queries. Valid values are from 1 to 5 seconds, and the default value is 1 second.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MLD Snooping Querier for VLAN 3, and configure the query interval as 100 seconds:

```
Device(config)# ipv6 mld snooping vlan-config 3 querier
Device(config)# ipv6 mld snooping vlan-config 3 querier query interval
100
```

27.10 ipv6 mld snooping (interface)

Description

The **ipv6 mld snooping** command is used to enable MLD Snooping function on the desired port. To disable this function, please use **no ipv6 mld snooping** command.

Syntax

ipv6 mld snooping

no ipv6 mld snooping

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable MLD Snooping on port 1/0/3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# ipv6 mld snooping
```

27.11 ipv6 mld snooping max-groups

Description

The **ipv6 mld snooping max-groups** command is used to configure the maximum number of groups that a port can join in. The **ipv6 mld snooping max-groups action** is used to configure the action that the port takes when it receives an MLD report message and the maximum number of entries is in

the forwarding table. To remove the maximum group limitation and return to the default of no limitation on the specified port, please use the **no ipv6 mld snooping max-groups** command. To return to the default action of dropping the report, please use the **no ipv6 mld snooping max-groups action** command. These commands only apply to the dynamic multicast groups.

Syntax

ipv6 mld snooping max-groups *maxgroup*

ipv6 mld snooping max-groups action { drop | replace }

no ipv6 mld snooping max-groups

no ipv6 mld snooping max-groups action

Parameter

maxgroup —— Specify the maximum numbers of groups that the port can join. It ranges from 0 to 1000 and the default value is 1000.

drop —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the port will not join any new multicast group.

replace —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the maximum numbers of groups that ports 1/0/2-5 can join as 10, and configure the throttling action as replace:

Device(config)#interface range gigabitEthernet 1/0/2-5

Device(config-if-range)#ipv6 mld snooping max-groups 10

Device(config-if-range)#ipv6 mld snooping max-groups action replace

27.12 ipv6 mld snooping immediate-leave

Description

The **ipv6 mld snooping immediate-leave** command is used to configure the Fast Leave function for port. To disable the Fast Leave function, please use **no ipv6 mld snooping immediate-leave** command.

Syntax

ipv6 mld snooping immediate-leave

no ipv6 mld snooping immediate-leave

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the Fast Leave function for port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# ipv6 mld snooping immediate-leave

27.13 ipv6 mld profile

Description

The **ipv6 mld profile** command is used to create the configuration profile. To delete the corresponding profile, please use **no ipv6 mld profile** command.

Syntax

ipv6 mld profile *id*

no ipv6 mld profile *id*

Parameter

id—— Specify the id of the configuration profile, ranging from 1 to 999.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Create the profile 1:

```
Device(config)# ipv6 mld profile 1
```

27.14 deny

Description

The **deny** command is used to configure the filtering mode of profile as deny.

Syntax

deny

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the filtering mode of profile 1 as deny:

```
Device(config)# ipv6 mld profile 1
Device(config-MLD-profile)#deny
```

27.15 permit

Description

The **permit** command is used to configure the filtering mode of profile as permit.

Syntax

permit

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the filtering mode of profile 1 as permit:

```
Device(config)# ipv6 mld profile 1
Device(config-igmp-profile)#permit
```

27.16 range

Description

The **range** command is used to configure the range of the profile's filtering multicast address. To delete the corresponding filtering multicast address, please use **no range** command. A profile contains 16 filtering IP-range entries at most.

Syntax

range *start-ip end-ip*

no range *start-ip end-ip*

Parameter

start-ip —— Start IPv6 multicast address of the filter entry..

end-ip —— End IPv6 multicast address of the filter entry.

Command Mode

Profile Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure one of the filter multicast address entry as range ff80::1234 to ff80::1235 in profile 1:

```
Device(config)# ipv6 mld profile 1
Device(config-igmp-profile)#range ff80::1234 ff80::1235
```

27.17 ipv6 mld filter

Description

The **ipv6 mld filter** command is used to bind the specified profile to the interface. To delete the binding, please use **no ipv6 mld filter** command.

Syntax

ipv6 mld filter *profile-id*

no ipv6 mld filter

Parameter

profile-id—— Specify the profile ID, ranging from 1 to 999.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Bind profile 1 to interface gigabitEthernet 1/0/2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# ipv6 mld filter 1
```

27.18 clear ipv6 mld snooping statistics

Description

The **clear ipv6 mld snooping statistics** command is used to clear the statistics of the MLD packets.

Syntax

clear ipv6 mld snooping statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the statistics of the MLD packets:

```
Device(config)# clear ipv6 mld snooping statistics
```

27.19 show ipv6 mld snooping

Description

The **show ipv6 mld snooping** command is used to display the global configuration of MLD Snooping.

Syntax

show ipv6 mld snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of MLD Snooping:

```
Device(config)# show ipv6 mld snooping
```

27.20 show ipv6 mld snooping interface

Description

The **show ipv6 mld snooping interface** command is used to display the port configuration of MLD snooping.

Syntax

show ipv6 mld snooping interface [gigabitEthernet [*port* | *port-list*]] { basic-config | max-groups | packet-stat }

show ipv6 mld snooping interface [port-channel [*port-channel-list*]] { basic-config | max-groups }

Parameter

port —— The Ethernet port number.

port-list —— The list of Ethernet ports.

basic-config | max-groups | packet-stat —— The related configuration information selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MLD baisic configuration configuration of all ports and port channels:

```
Device# show ipv6 mld snooping interface basic-config
```

Display the MLD basic configuration of port 1/0/2:

```
Device# show ipv6 mld snooping interface gigabitEthernet 1/0/2
basic-config
```

Display the MLD packet statistics of ports 1/0/1-4:

```
Device# show ipv6 mld snooping interface gigabitEthernet 1/0/1-4
packet-stat
```

27.21 show ipv6 mld snooping vlan

Description

The **show ipv6 mld snooping vlan** command is used to display VLAN information of MLD Snooping.

Syntax

show ipv6 mld snooping vlan [*vlan-id*]

Parameter

vlan-id—— The VLAN ID selected to display, ranging from 1 to 4094.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the VLAN information:

```
Device(config)# show ipv6 mld snooping vlan
```

27.22 show ipv6 mld snooping groups

Description

The **show ipv6 mld snooping groups** command is used to display multicast groups.

Syntax

show ipv6 mld snooping groups [vlan { *vlan-id*}] [*ipv6_multicast_addr* | count | dynamic | dynamic count | static | static count]

Parameter

vlan-id——The VLAN ID selected to display the information of all multicast items.

ipv6_multicast_addr —— IPv6 address of the multicast group.

count—— The numbers of all multicast groups.

dynamic—— Display dynamic multicast groups.

dynamic count—— The numbers of all dynamic multicast groups.

static—— Display static multicast groups.

static count—— The numbers of all static multicast groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the multicast groups:

```
Device(config)# show ipv6 mld snooping groups
```

27.23 show ipv6 mld profile

Description

The **show ipv6 mld profile** command is used to display the configuration information of all the profiles or a specific profile.

Syntax

show ipv6 mld profile [*id*]

Parameter

id —— Specify the ID of the profile, ranging from 1 to 999.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of all profiles:

```
Device(config)# show ipv6 mld profile
```

Chapter 28 MVR Commands

MVR (Multicast VLAN Registration) allows a single multicast VLAN to be shared for multicast member ports in different VLANs in IPv4 network. In IGMP Snooping, if member ports are in different VLANs, a copy of the multicast streams is sent to each VLAN that has member ports. While MVR provides a dedicated multicast VLAN to forward multicast traffic over the Layer 2 network, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs.

28.1 mvr (global)

Description

The **mvr** command is used to enable MVR globally. To disable MVR, please use **no mvr** command.

Syntax

mvr

no mvr

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MVR globally:

```
Device(config)# mvr
```

28.2 mvr group

Description

The **mvr group** command is used to add multicast groups to MVR. To delete multicast groups from MVR, please use **no mvr group** command. You can configure up to 511 multicast groups.

Syntax

mvr group *ip-addr* [*count*]

no mvr group *ip-addr* [*count*]

Parameter

ip-addr —— The start IP address of the contiguous series of multicast groups.

count —— The number of the multicast groups to be added to the MVR. Valid values are from 1 to 256, and the default value is 1.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add multicast groups 225.1.2.3 -239.1.2.5 to MVR:

Device (config)# mvr group 225.1.2.3 3

28.3 mvr mode

Description

The **mvr mode** command is used to configure the MVR mode as compatible or dynamic. By default, it is compatible. To return to the default configuration, please use **no mvr mode** command.

Syntax

mvr mode {compatible | dynamic}

no mvr mode

Parameter

compatible —— In this mode, the device does not forward report or leave messages from the hosts to the IGMP querier. So the IGMP querier cannot learn the multicast groups membership information from the device. You have to statically configure the IGMP querier to transmit all the required multicast streams to the device via the multicast VLAN.

dynamic —— In this mode, after receiving report or leave messages from the hosts, the device will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). So the IGMP querier can learn the multicast groups membership information through the report and leave messages, and transmit the multicast streams to the device via the multicast VLAN according to the multicast forwarding table.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MVR mode as dynamic:

```
Device(config)# mvr mode dynamic
```

28.4 mvr querytime

Description

The **mvr querytime** command is used to configure the maximum time to wait for IGMP report on a receiver port before removing the port from multicast group membership. To return to the default configuration, please use **no mvr querytime** command.

Syntax

mvr querytime *time*

no mvr querytime

Parameter

time —— The query response time. Valid values are from 1 to100 tenths of a second, and the default value is 5 tenths of a second.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the query response time of MVR as 1 second, that is 10 tenths of a second:

```
Device(config)# mvr querytime 10
```

28.5 mvr vlan

Description

The **mvr vlan** command is used to specify the multicast VLAN. By default, it is VLAN 1. To return to the default configuration, please use **no mvr vlan** command.

Syntax

mvr vlan *vlan-id*

no mvr vlan

Parameter

vlan-id—— The ID of the multicast VLAN. Valid values are from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the multicast VLAN as VLAN 10:

```
Device(config)# mvr vlan 10
```

28.6 mvr (interface)

Description

This command is used to enable MVR for specific interfaces. To disable MVR for the interfaces, please use **no mvr** command. By default, it is disabled.

Syntax

mvr

no mvr

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable MVR for port 1/0/1:

Device(config)# interface gigabitEthernet 1/0/1

Device(config-if)#mvr

28.7 mvr type

Description

The **mvr type** command is used to configure the MVR port type as receiver or source. By default, the port is a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation fails. To return to the default configuration, please use **no mvr type** command.

Syntax

mvr type {source | receiver}

no mvr type

Parameter

source —— Configure the uplink ports that receive and send multicast data on the multicast VLAN as source ports. Source ports should belong to the multicast VLAN. When the interface configuration mode is interface gigabitEthernet, only **mvr type** source can be input.

receiver —— Configure the ports that are connecting to the hosts as receiver ports. A receiver port can only belong to one VLAN, and cannot belong to the multicast VLAN. When the interface configuration mode is interface gpon, only **mvr type** receiver can be input.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernetl)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the port 1/0/3 as a receiver port:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)#mvr type receiver
```

28.8 mvr immediate

Description

The **mvr immediate** command is used to enable the Fast Leave feature of MVR for specified port. To disable the Fast Leave feature of MVR for specific ports, please use **no mvr immediate** command.

Syntax

mvr immediate

no mvr immediate

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernetl)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Only receiver ports support Fast Leave. Before enabling Fast Leave for a port, make sure there is only a single receiver device connecting to the port.

Example

Enable the Fast Leave feature of MVR for port 1/0/3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)#mvr immediate
```

28.9 mvr vlan (group)

Description

This command is used to statically add ports to an MVR group. Then the ports can receive multicast traffic sent to the IP multicast address via the multicast VLAN.

Syntax

mvr vlan *vlan-id* **group** *ip-addr*

Parameter

vlan-id —— The ID of the multicast VLAN. Valid values are from 1 to 4094.

ip-addr —— The IP address of the multicast group.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon / interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernetl)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

This command applies to only receiver ports. The device adds or removes the receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts. You can also statically add a receiver port to an MVR group.

Example

Add port 1/0/3 to MVR group 225.1.2.3 statically. The multicast VLAN is VLAN 10:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)#mvr vlan 10 group 225.1.2.3
```

28.10 show mvr

Description

The **show mvr** command is used to display the global configuration of MVR.

Syntax

show mvr

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of mvr:

```
Device# show mvr
```

28.11 show mvr interface

Description

The **show mvr interface** command is used to display the MVR configurations of specific interfaces.

Syntax

show mvr interface gigabitEthernet [*port* | *port-list*]

Parameter

port——The Ethernet port number.

port-list—— The list of Ethernet ports.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MVR configuration of port 1/0/3:

```
Device# show mvr interface gigabitEthernet 1/0/3
```

28.12 show mvr members

Description

The **show mvr members** command is used to display the membership information of all MVR groups or the specified MVR group.

Syntax

show mvr members [*ip-addr*] [status {active | inactive}]

Parameter

ip-addr——The multicast IP address of the MVR group.

active—— Display all active MVR groups.

inactive——Display all inactive MVR groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the membership information of all MVR groups:

```
Device# show mvr members
```

Chapter 29 MSTP Commands

MSTP (Multiple Spanning Tree Protocol), compatible with both STP and RSTP and subject to IEEE 802.1s, can disbranch a ring network. STP is to block redundant links and backup links as well as optimize paths.

29.1 debug spanning-tree

Description

The **debug spanning-tree** command is used to enable debuggning of spanning-tree activities. To disable the debugging function, please use **no debug spanning-tree** command.

Syntax

debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

no debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

Parameters

all —— Display all the spanning-tree debug messages.

bpdu receive —— Display the debug messages of the received spanning-tree bridge protocol data unit (BPDU).

bpdu transmit —— Display the debug messages of the sent spanning-tree BPDU.

cmpmsg —— Display the message priority debug messages.

errors —— Display the MSTP error debug messages.

flush —— Display the address table flushing debug messages.

init —— Display the data structure initialization debug messages.

migration —— Display the version migration debug messages.

proposals —— Display the MSTP handshake debug messages.

roles —— Display the MSTP interface role switchling debug messages.

state —— Display the MSTP interface state change debug messages.

tc —— Display the MSTP topology event debug messages.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display all the spanning-tree debug messages:

```
Device# debug spanning-tree all
```

29.2 spanning-tree (global)

Description

The **spanning-tree** command is used to enable STP function globally. To disable the STP function, please use **no spanning-tree** command.

Syntax

spanning-tree

no spanning-tree

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the STP function:

```
Device(config)# spanning-tree
```

29.3 spanning-tree (interface)

Description

The **spanning-tree** command is used to enable STP function for a port. To disable the STP function, please use **no spanning-tree** command.

Syntax

spanning-tree

no spanning-tree

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the STP function for port 1/0/2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree
```

29.4 spanning-tree common-config

Description

The **spanning-tree common-config** command is used to configure the parameters of the ports for comparison in the CIST and the common parameters of all instances. To return to the default configuration, please use **no spanning-tree common-config** command. CIST (Common and Internal Spanning Tree) is the spanning tree in a switched network, connecting all devices in the network.

Syntax

spanning-tree common-config [port-priority *pri*] [ext-cost *ext-cost*] [int-cost *int-cost*] [portfast { enable | disable }] [point-to-point { auto | open | close }]

no spanning-tree common-config

Parameter

pri—— Port Priority, which must be multiple of 16 ranging from 0 to 240. By default, the port priority is 128. Port Priority is an important criterion on determining if the port connected to this port will be chosen as the root port. In the same condition, the port with the highest priority will be chosen as the root port. The lower value has the higher priority.

ext-cost—— External Path Cost, which is used to choose the path and calculate the path costs of ports in different MST regions. It is an important criterion on determining the root port. The lower value has the higher priority. It ranges from o to 2000000. By default, it is 0 which is mean auto.

int-cost—— Internal Path Cost, which is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on determining the root port. The lower value has the higher priority. By

default, it is automatic. It ranges from o to 2000000. By default, it is 0 which is mean auto.

portfast —— Enable/ Disable Edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding rapidly without waiting for forward delay.

point-to-point —— The P2P link status, with auto, open and close options. By default, the option is auto. If the two ports in the P2P link are root port or designated port, they can transit their states to forwarding rapidly to reduce the unnecessary forward delay.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the STP function of port 1, and configure the Port Priority as 64, ExtPath Cost as 100, IntPath Cost as 100, and then enable Edge Port:

Device(config)# interface gigabitEthernet 1/0/1

Device(config-if)# spanning-tree common-config port-priority 64

ext-cost 100 **int-cost** 100 **portfast** enable **point-to-point** open

29.5 spanning-tree mode

Description

The **spanning-tree mode** command is used to configure the STP mode of the device. To return to the default configurations, please use **no spanning-tree mode** command.

Syntax

spanning-tree mode { stp | rstp | mstp }

no spanning-tree mode

Parameter

stp ——Spanning Tree Protocol, the default value.

rstp ——Rapid Spanning Tree Protocol

mstp ——Multiple Spanning Tree Protocol

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the spanning-tree mode as mstp:

```
Device(config)# spanning-tree mode mstp
```

29.6 spanning-tree mst configuration

Description

The **spanning-tree mst configuration** command is used to access MST Configuration Mode from Global Configuration Mode, as to configure the VLAN-Instance mapping, region name and revision level. To return to the default configuration of the corresponding Instance, please use **no spanning-tree mst configuration** command.

Syntax

spanning-tree mst configuration

no spanning-tree mst configuration

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enter into the MST configuration mode:

```
Device(config)# spanning-tree mst configuration
Device(Config-mst)#
```

29.7 instance

Description

The **instance** command is used to configure the VLAN-Instance mapping. To remove the VLAN-instance mapping or disable the corresponding instance,

please use **no instance** command. When an instance is disabled, the related mapping VLANs will be removed.

Syntax

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

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

Parameters

instance-id—— Instance ID, ranging from 1 to 32.

vlan-id—— The VLAN ID selected to mapping with the corresponding instance.

Command Mode

MST Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Map the VLANs 1-100 to Instance 1:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 1 vlan 1-100
```

Disable Instance 1, namely remove all the mapping VLANs 1-100:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 1
```

Remove VLANs 1-50 in mapping VLANs 1-100 for Instance 1:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# no instance 1 vlan 1-50
```

29.8 name

Description

The **name** command is used to configure the region name of MST instance.

Syntax

name *name*

Parameters

name —— The region name, used to identify MST region. It ranges from 1 to 32 characters.

Command Mode

MST Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the region name of MST as “region1”:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# name region1
```

29.9 revision

Description

The **revision** command is used to configure the revision level of MST instance.

Syntax

revision *revision*

Parameters

revision —— The revision level for MST region identification, ranging from 0 to 65535.

Command Mode

MST Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the revision level of MST as 100:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# revision 100
```

29.10 spanning-tree mst instance

Description

The **spanning-tree mst instance** command is used to configure the priority of MST instance. To return to the default value of MST instance priority, please use **no spanning-tree mst instance** command.

Syntax

spanning-tree mst instance *instance-id* **priority** *pri*

no spanning-tree mst instance *instance-id* **priority**

Parameter

instance-id—— Instance ID, ranging from 1 to 8.

pri—— MSTI Priority, which must be multiple of 4096 ranging from 0 to 61440. By default, it is 32768. MSTI priority is an important criterion on determining if the device will be chosen as the root bridge in the specific instance.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MST Instance 1 and configure its priority as 4096:

```
Device(config)# spanning-tree mst instance 1 priority 4096
```

29.11 spanning-tree mst

Description

The **spanning-tree mst** command is used to configure MST Instance Port. To return to the default configuration of the corresponding Instance Port, please use **no spanning-tree mst** command. A port can play different roles in different spanning tree instance. You can use this command to configure the parameters of the ports in different instance IDs as well as view status of the ports in the specified instance.

Syntax

spanning-tree mst instance *instance-id* {[port-priority *pri*] | [cost *cost*]}

no spanning-tree mst instance *instance-id*

Parameter

instance-id—— Instance ID, ranging from 1 to 8.

pri—— Port Priority, which must be multiple of 16 ranging from 0 to 240. By default, it is 128. Port Priority is an important criterion on determining if the port will be chosen as the root port by the device connected to this port.

cost—— Path Cost, ranging from 0 to 200000. The lower value has the higher priority. Its default value is 0 meaning "auto".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the priority of port 1 in MST Instance 1 as 64, and path cost as 2000:

```
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# spanning-tree mst instance 1 port-priority 64 cost
2000
```

29.12 spanning-tree priority

Description

The **spanning-tree priority** command is used to configure the bridge priority. To return to the default value of bridge priority, please use **no spanning-tree priority** command.

Syntax

spanning-tree priority *pri*

no spanning-tree priority

Parameter

pri—— Bridge priority, ranging from 0 to 61440. It is 32768 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the bridge priority as 4096:

```
Device(config)# spanning-tree priority 4096
```

29.13 spanning-tree timer

Description

The **spanning-tree timer** command is used to configure forward-time, hello-time and max-age of Spanning Tree. To return to the default configurations, please use **no spanning-tree timer** command.

Syntax

spanning-tree timer {[forward-time *forward-time*] [hello-time *hello-time*] [max-age *max-age*]}

no spanning-tree timer

Parameter

forward-time —— Forward Delay, which is the time for the port to transit its state after the network topology is changed. Forward Delay ranges from 4 to 30 in seconds and it is 15 by default. Otherwise, 2 * (Forward Delay - 1) >= Max Age.

hello-time ——Hello Time, which is the interval to send BPDU packets, and used to test the links. Hello Time ranges from 1 to 10 in seconds and it is 2 by default. Otherwise, 2 * (Hello Time + 1) <= Max Age.

max-age —— The maximum time the device can wait without receiving a BPDU before attempting to reconfigure, ranging from 6 to 40 in seconds. By default, it is 20.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure forward-time, hello-time and max-age for Spanning Tree as 16 seconds, 3 seconds and 22 seconds respectively:

Device(config)# spanning-tree timer forward-time 16 **hello-time** 3 **max-age** 22

29.14 spanning-tree hold-count

Description

The **spanning-tree hold-count** command is used to configure the maximum number of BPDU packets transmitted per Hello Time interval. To return to the default configurations, please use **no spanning-tree hold-count** command.

Syntax

spanning-tree hold-count *value*

no spanning-tree hold-count

Parameter

value —— The maximum number of BPDU packets transmitted per Hello Time interval, ranging from 1 to 20 in pps. By default, it is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the hold-count of STP as 8pps:

Device(config)# spanning-tree hold-count 8

29.15 spanning-tree max-hops

Description

The **spanning-tree max-hops** command is used to configure the maximum number of hops that occur in a specific region before the BPDU is discarded. To return to the default configurations, please use **no spanning-tree max-hops** command.

Syntax

spanning-tree max-hops *value*

no spanning-tree max-hops

Parameter

value —— The maximum number of hops that occur in a specific region before the BPDU is discarded, ranging from 1 to 40 in hop. By default, it is 20.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the max-hops of STP as 30:

```
Device(config)# spanning-tree max-hops 30
```

29.16 spanning-tree bpdufilter

Description

The **spanning-tree bpdufilter** command is used to enable the BPDU filter function for a port. With the BPDU Filter function enabled, the port does not forward BPDUs from the other devices. To disable the BPDU filter function, please use **no spanning-tree bpdufilter** command.

Syntax

spanning-tree bpdufilter

no spanning-tree bpdufilter

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BPDU filter function for port 1/0/2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree bpdufilter
```

29.17 spanning-tree bpduflood

Description

The **spanning-tree bpduflood** command is used to enable the BPDU forward function for a port. With the function enabled, the port still can forward spanning tree BPDUs when the spanning tree function is disabled on this port. To disable the BPDU filter function, please use **no spanning-tree bpduflood** command.

Syntax

spanning-tree bpduflood

no spanning-tree bpduflood

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BPDU forward function for port 1/0/2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree bpduflood
```

29.18 spanning-tree bpduguard

Description

The **spanning-tree bpduguard** command is used to enable the BPDU protect function for a port. With the BPDU protect function enabled, the port will set itself automatically as ERROR-PORT when it receives BPDU packets, and the port will disable the forwarding function for a while. To disable the BPDU protect function, please use **no spanning-tree bpduguard** command.

Syntax

spanning-tree bpduguard

no spanning-tree bpduguard

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the BPDU protect function for port 1/0/2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree bpduguard
```

29.19 spanning-tree guard loop

Description

The **spanning-tree guard loop** command is used to enable the Loop Protect function for a port. Loop Protect is to prevent the loops in the network brought by recalculating STP because of link failures and network congestions. To disable the Loop Protect function, please use **no spanning-tree guard loop** command.

Syntax

spanning-tree guard loop

no spanning-tree guard loop

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Loop Protect function for port 2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree guard loop
```

29.20 spanning-tree guard root

Description

The **spanning-tree guard root** command is used to enable the Root Protect function for a port. With the Root Protect function enabled, the root bridge will set itself automatically as ERROR-PORT when receiving BPDU packets with higher priority, in order to maintain the role of root ridge. To disable the Root Protect function, please use **no spanning-tree guard root** command.

Syntax

spanning-tree guard root

no spanning-tree guard root

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Root Protect function for port 2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree guard root
```

29.21 spanning-tree guard tc

Description

The **spanning-tree guard tc** command is used to enable the TC Protect of Spanning Tree function for a port. To disable the TC Protect of Spanning Tree function, please use **no spanning-tree guard tc** command. A device removes MAC address entries upon receiving TC-BPDUs. If a malicious user continuously sends TC-BPDUs to a device, the device will be busy with removing MAC address entries, which may decrease the performance and stability of the network. With the Protect of Spanning Tree function enabled, you can configure the number of TC-BPDUs in a required time, so as to avoid the process of removing MAC addresses frequently.

Syntax

spanning-tree guard tc

no spanning-tree guard tc

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the TC Protect of Spanning Tree for port 2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree guard tc
```

29.22 spanning-tree mcheck

Description

The **spanning-tree mcheck** command is used to enable mcheck.

Syntax

spanning-tree mcheck

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable mcheck for port 2:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# spanning-tree mcheck
```

29.23 show spanning-tree active

Description

The **show spanning-tree active** command is used to display the active information of spanning-tree.

Syntax

show spanning-tree active

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the active information of spanning-tree:

```
Device(config)# show spanning-tree active
```

29.24 show spanning-tree bridge

Description

The **show spanning-tree bridge** command is used to display the bridge parameters.

Syntax

show spanning-tree bridge [forward-time | hello-time | hold-count | max-age | max-hops | mode | priority | state]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bridge parameters:

```
Device(config)# show spanning-tree bridge
```

29.25 show spanning-tree interface

Description

The **show spanning-tree interface** command is used to display the spanning-tree information of all ports or a specified port.

Syntax

show spanning-tree interface [gigabitEthernet *port* | port-channel *port-channel-id*] [edge | ext-cost | int-cost | mode | p2p | priority | role | state | status]

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the spanning-tree information of all ports:

Device(config)# show spanning-tree interface

Display the spanning-tree information of port 1/0/2:

Device(config)# show spanning-tree interface gigabitEthernet 1/0/2

Display the spanning-tree mode information of port 1/0/2:

Device(config)# show spanning-tree interface gigabitEthernet 1/0/2 mode

29.26 show spanning-tree interface-security

Description

The **show spanning-tree interface-security** command is used to display the protect information of all ports or a specified port.

Syntax

show spanning-tree interface-security [gigabitEthernet *port* | port-channel *port-channel-id*] [bpdufilter | bpduflood | bpduguard | loop | root | tc]

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the protect information of all ports:

Device(config)# show spanning-tree interface-security

Display the protect information of port 1:

Device(config)# show spanning-tree interface-security gigabitEthernet 1/0/1

Display the interface security bpdufilter information:

Device(config)# show spanning-tree interface-security bpdufilter

29.27 show spanning-tree mst

Description

The **show spanning-tree mst** command is used to display the related information of MST Instance.

Syntax

show spanning-tree mst { configuration [digest] | instance *instance-id* [interface [gigabitEthernet *port* | port-channel *port-channel-id*]] }

Parameter

instance-id—— Instance ID desired to show, ranging from 1 to 8.

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the region information and mapping information of VLAN and MST Instance:

Device(config)#show spanning-tree mst configuration

Display the related information of MST Instance 1:

Device(config)#show spanning-tree mst instance 1

Display all the ports information of MST Instance 1:

Device(config)#show spanning-tree mst instance 1 **interface**

Chapter 30 LLDP Commands

LLDP function enables network devices to advertise their own device information periodically to neighbors on the same LAN. The information of the LLDP devices in the LAN can be stored by its neighbor in a standard MIB, so it is possible for the information to be accessed by a Network Management System (NMS) using SNMP.

30.1 lldp

Description

The **lldp** command is used to enable LLDP function. To disable the LLDP function, please use **no lldp** command.

Syntax

lldp

no lldp

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable LLDP function globally:

```
Device(config)#lldp
```

30.2 lldp forward_message

Description

The **lldp forward_message** command is used to enable the device to forward LLDP messages when LLDP function is disabled. To disable the LLDP messages forwarding function, please use **no lldp forward_message** command.

Syntax

lldp forward_message

no lldp forward_message

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the device to forward LLDP messages when LLDP function is disabled globally:

Device(config)#lldp forward_message

30.3 lldp hold-multiplier

Description

The **lldp hold-multiplier** command is used to configure the Hold Multiplier parameter. The aging time of the local information in the neighbor device is determined by the actual TTL value used in the sending LLDPDU. TTL = Hold Multiplier * Transmit Interval. To return to the default configuration, please use **no lldp hold-multiplier** command.

Syntax

lldp hold-multiplier *multiplier*

no lldp hold-multiplier

Parameter

multiplier —— Configure the Hold Multiplier parameter. It ranges from 2 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify Hold Multiplier as 5:

Device(config)#lldp hold-multiplier 5

30.4 lldp timer

Description

The **lldp timer** command is used to configure the parameters about transmission. To return to the default configuration, please use **no lldp timer** command.

Syntax

lldp timer { tx-interval *tx-interval* | tx-delay *tx-delay* | reinit-delay *reinit-delay* | notify-interval *notify-interval* | fast-count *fast-count* }

no lldp timer { tx-interval | tx-delay | reinit-delay | notify-interval | fast-count }

Parameter

tx-interval —— Configure the interval for the local device to transmit LLDPDU to its neighbors. The value ranges from 5 to 32768 and the default value is 30 seconds.

tx-delay —— Configure a value from 1 to 8192 in seconds to specify the time for the local device to transmit LLDPDU to its neighbors after changes occur so as to prevent LLDPDU being sent frequently. By default, it is 2 seconds.

reinit-delay —— This parameter indicates the amount of delay from when LLDP status becomes "disable" until re-initialization will be attempted. The value ranges from 1 to 10 and the default value is 2.

notify-interval —— Specify the interval of Trap message which will be sent from local device to network management system. The value ranges from 5 to 3600 and the default value is 5 seconds.

fast-count —— When the port's LLDP state transforms from Disable (or Rx_Only) to Tx&Rx (or Tx_Only), the fast start mechanism will be enabled, that is, the transmit interval will be shorten to a second, and several LLDPDUs will be sent out (the number of LLDPDUs equals this parameter). The value ranges from 1 to 10 and the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the Transmit Interval of LLDPDU as 45 seconds and Trap message to NMS as 120 seconds:

Device(config)#lldp timer tx-interval 45

Device(config)#lldp timer notify-interval 120

30.5 lldp receive

Description

The **lldp receive** command is used to enable the designated port to receive LLDPDU. To disable the function, please use **no lldp receive** command.

Syntax

lldp receive

no lldp receive

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable port 1/0/1 to receive LLDPDU:

Device(config)#interface gigabitEthernet 1/0/1

Device(config-if)#lldp receive

30.6 lldp transmit

Description

The **lldp transmit** command is used to enable the designated port to transmit LLDPDU. To disable the function, please use **no lldp transmit** command.

Syntax

lldp transmit

no lldp transmit

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable Gigabit Ethernet port 1/0/1 to transmit LLDPDU:

```
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)#lldp transmit
```

30.7 lldp snmp-trap

Description

The **lldp snmp-trap** command is used to enable the port's SNMP notification. If enabled, the port will notify the trap event to network management system. To disable the ports' SNMP notification, please use **no lldp snmp-trap** command.

Syntax

lldp snmp-trap

no lldp snmp-trap

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the SNMP notification for Gigabit Ethernet port 1/0/1:

```
Device(config)#interface gigabitEthernet 1/0/1
Device(config-if)#lldp snmp-trap
```

30.8 lldp tlv-select

Description

The **lldp tlv-select** command is used to configure TLVs to be included in outgoing LLDPDU. To exclude TLVs, please use **no lldp tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

lldp tlv-select { [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all] }

no lldp tlv-select { [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all] }

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Exclude “management-address” and “port-vlan-id” TLVs in LLDPDU outgoing from Gigabit Ethernet port 1/0/1:

```
Device(config)# interface gigabitEthernet 1/0/1

Device(config-if)# no lldp tlv-select management-address port-vlan
```

30.9 lldp management-address

Description

The **lldp management-address** command is used to configure the port‘s management address to be included in management address TLV. The NMS uses management addresses to identify the devices. To delete the port‘s management address, please use **no lldp management address** command.

Syntax

lldp management-address { *ip-address* }

no lldp management-address

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the port's management address as 192.168.1.100 for port 1/0/1:

Device(config)# interface gigabitEthernet 1/0/1

Device(config-if)# lldp management-address 192.168.0.100

30.10 lldp med-fast-count

Description

The **lldp med-fast-count** command is used to configure the number of the LLDP-MED frames that will be sent out. When LLDP-MED fast start mechanism is activated, multiple LLDP-MED frames will be transmitted based on this parameter. The default value is 4. To return to the default configuration, please use **no lldp med-fast-count** command.

Syntax

lldp med-fast-count *count*

no lldp med-fast-count

Parameter

count—— Configure the Fast Start Count parameter. It ranges from 1 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify Fast Start Count as 5:

Device(config)# lldp med-fast-count 5

30.11 lldp med-status

Description

The **lldp med-status** command is used to enable the LLDP-MED feature for the corresponding port. After the LLDP-MED feature is enabled, the port's Admin Status will be changed to Tx&Rx. To disable the LLDP-MED feature for the corresponding port, please use **no lldp med-status** command.

Syntax

lldp med-status

no lldp med-status

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the LLDP-MED feature for port 1/0/2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# lldp med-status

30.12 lldp med-tlv-select

Description

The **lldp med-tlv-select** command is used to configure LLDP-MED TLVs to be included in outgoing LLDPDU for the corresponding port. To exclude LLDP-MED TLVs, please use **no lldp med-tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }

no lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Exclude "network policy" and "inventory" TLVs in LLDPDU outgoing from port 1/0/2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# no lldp med-tlv-select network-policy inventory-management

30.13 lldp med-location

Description

The lldp med-location command is used to configure the Location Identification TLV's content in outgoing LLDPDU of the port.

Syntax

lldp med-location { emergency-number *identifier* | civic-address [[language *language*] [province-state *province-state*] [lci-county-name *county-name*] [lci-city *city*] [street *street*] [house-number *house-number*] [name *name*] [postal-zipcode *postal-zipcode*] [room-number *room-number*] [post-office-box *post-office-box*] [additional *additional*] [country-code *country-code*] [what { dhcp-server | endpoint | switch }]] }

Parameter

emergency-number —— Emergency Call Service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The length of this field ranges from 10 to 25 characters.

civic-address —— The civic address is defined to reuse the relevant sub-fields of the DHCP option for civic Address based Location Configuration Information as specified by IETF.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the civic address in the Location Identification TLV's content in outgoing LLDPDU of port 1/0/2. Configure the language as English and city as London:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# lldp med-location civic-address language English lci-city London
```

30.14 show lldp

Description

The **show lldp** command is used to display the global configuration of LLDP.

Syntax

show lldp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of LLDP:

```
Device#show lldp
```

30.15 show lldp interface

Description

The **show lldp interface** command is used to display LLDP configuration of the corresponding port. By default, the LLDP configuration of all the ports will be displayed.

Syntax

show lldp interface [gigabitEthernet *port*]

Parameters

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP configuration of Gigabit Ethernet port 1/0/1:

Device#show lldp interface gigabitEthernet 1/0/1

30.16 show lldp local-information interface

Description

The **show lldp local-information interface** command is used to display the LLDP information of the corresponding port. By default, the LLDP information of all the ports will be displayed.

Syntax

show lldp local-information interface [gigabitEthernet *port*]

Parameters

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP information of 1/0/1:

Device#show lldp local-information interface gigabitEthernet 1/0/1

30.17 show lldp neighbor-information interface

Description

The **show lldp neighbor-information interface** command is used to display the neighbor information of the corresponding port. By default, the neighbor information of all the ports will be displayed.

Syntax

show lldp neighbor-information interface [gigabitEthernet *port*]

Parameters

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the neighbor information of Gigabit Ethernet port 1/0/1:

Device#show lldp neighbor-information interface gigabitEthernet 1/0/1

30.18 show lldp traffic interface

Description

The **show lldp traffic interface** command is used to display the LLDP statistic information between the local device and neighbor device of the corresponding port. By default, the LLDP statistic information of all the ports will be displayed.

Syntax

show lldp traffic interface [gigabitEthernet *port*]

Parameters

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP statistic information of Gigabit Ethernet port 1/0/1:

Device#show lldp traffic interface gigabitEthernet 1/0/1

Chapter 31 Static Routes Commands

31.1 ip routing

Description

This **ip routing** command is used to enable IPv4 routing globally. To disable IPv4 routing, please use the **no ip routing** command.

Syntax

ip routing

no ip routing

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IPv4 routing feature for the device:

```
Device(config)# ip routing
```

31.2 interface vlan

Description

This **interface vlan** command is used to create the VLAN interface. To delete the specified VLAN interface, please use the **no interface vlan** command.

Syntax

interface vlan { *vid*}

no interface vlan { *vid*}

Parameter

vid—— The ID of the VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the VLAN interface 2:

```
Device(config)# interface vlan 2
```

31.3 interface loopback

Description

This **interface loopback** command is used to create the loopback interface. To delete the specified loopback interface, please use the **no interface loopback** command.

Syntax

interface loopback { *id*}

no interface loopback { *id*}

Parameter

id—— The ID of the loopback interface, ranging from 1 to 64.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the loopback interface 1:

```
Device(config)# interface loopback 1
```

31.4 switchport

Description

This **switchport** command is used to switch the Layer 3 interface into the Layer 2 port. To switch the Layer 2 port into the Layer 3 routed port, please use the **no switchport** command.

Syntax

switchport

no switchport

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Device port 1/0/9 into the routed port:

Device(config)# interface gigabitEthernet 1/0/9
Device(config-if)# no switchport

31.5 interface range port-channel

Description

This **interface range port-channel** command is used to create multiple port-channel interfaces.

Syntax

interface range port-channel *port-channel-list*

Parameter

port-channel-list —— The list of the port-channel interface, ranging from 1 to 14, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the port-channel interfaces 1, 3, 4 and 5:

Device(config)# interface port-channel 1,3-5

31.6 description

Description

This **description** command is used to add a description to the Layer 3 interface, including routed port, port-channel interface, loopback interface and VLAN interface. To clear the description of the corresponding interface, please use the **no description** command.

Syntax

description *string*

no description

Parameter

string —— Content of an interface description, ranging from 1 to 32 characters.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add a description system-if to the routed port 1/0/9 :

```
Device(config)# interface gigabitEthernet 1/0/9
Device(config-if)# no switchport
Device(config-if)# description system-if
```

31.7 shutdown

Description

This **shutdown** command is used to shut down the specified interface. The interface type include: routed port, port-channel interface, loopback interface and VLAN interface. To enable the specified interface, please use the **no shutdown** command.

Syntax

shutdown

no shutdown

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Shut down the routed port 1/0/9:

```
Device(config)# interface gigabitEthernet 1/0/9
Device(config-if)# no switchport
Device(config-if)# shutdown
```

31.8 interface port-channel

Description

This **interface port-channel** command is used to create the port-channel interface. To delete the specified port-channel interface, please use the **no interface port-channel** command.

Syntax

interface port-channel { *port-channel-id*}

no interface port-channel { *port-channel-id*}

Parameter

port-channel-id—— The ID of the port-channel interface, ranging from 1 to 14.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the port-channel interface 1:

```
Device(config)# interface port-channel 1
```

31.9 ip route

Description

This **ip route** command is configure the static route. To clear the corresponding entry, please use the **no ip route** command.

Syntax

ip route { *dest-address* } { *mask* } { *next-hop-address* } [*distance*]

no ip route { *dest-address* } { *mask* } { *next-hop-address* }

Parameter

dest-address —— The destination IP address.

mask —— The subnet mask.

next-hop-address —— The address of the next-hop.

distance —— The distance metric of this route, ranging from 1 to 255. The smaller the distance is, the higher the priority is.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a static route with the destination IP address as 192.168.2.0, the subnet mask as 255.255.255.0 and the next-hop address as 192.168.0.2:

Device(config)# ip route 192.168.2.0 255.255.255.0 192.168.0.2

31.10 ipv6 routing

Description

This **ipv6 routing** command is enale the IPv6 routing feature globally. To diable IPv6 routing, please use the **no ipv6 routing** command.

Syntax

ipv6 routing

no ipv6 routing

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable IPv6 routing globally:

Device(config)# ipv6 routing

31.11 ipv6 route

Description

This **ipv6 route** command is configure the IPv6 static route. To clear the corresponding entry, please use the **no ipv6 route** command.

Syntax

ipv6 route { *ipv6-dest-address* } { *next-hop-address* } [*distance*]

no ipv6 route { *ipv6-dest-address* } { *next-hop-address* }

Parameter

ipv6-dest-address—— The IPv6 address of the destination network.

next-hop-address —— The IPv6 address of the next-hop.

distance —— The distance metric of this route, ranging from 1 to 255. The smaller the distance is, the higher the priority is.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a static route with the destination network IP address as 3200::/64 and the next-hop address as 3100::1234:

Device(config)# ipv6 route 3200::/64 3100::1234

31.12 show interface vlan

Description

The **show interface vlan** command is used to display the information of the specified interface VLAN.

Syntax

show interface vlan *vid*

Parameter

vid—— The VLAN ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of VLAN 2:

```
Device(config)#show interface vlan 2
```

31.13 show ip interface

Description

This **show ip interface** command is used to display the detailed information of the specified Layer 3 interface.

Syntax

show ip interface [gigabitEthernet *port* /port-channel *port-channel-id* / loopback *id*| vlan *vlan-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel. Member ports in this port channel should all be routed ports.

id—— The loopback interface ID.

vlan-id—— The VLAN interface ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the detailed information of the VLAN interface 2:

Device(config)# show ip interface vlan 2

31.14 show ip interface brief

Description

This **show ip interface brief** command is used to display the summary information of the Layer 3 interfaces.

Syntax

show ip interface brief

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of the Layer 3 interfaces:

Device(config)# show ip interface brief

31.15 show ip route

Description

This **show ip route** command is used to display the route entries of the specified type.

Syntax

show ip route [static | connected]

Parameter

static | connected —— Specify the route type. If not specified, all types of route entries will be displayed.

static: The static routes.

connected: The connected routes.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the static routes:

Device(config)# show ip route static

31.16 show ip route specify

Description

This **show ip route specify** command is used to display the valid routing information to the specified IP address or network segments.

Syntax

show ip route specify { *ip* } [*mask*] [longer-prefixes]

Parameter

ip —— Specify the destination IP address.

mask —— Specify the destination IP address together with the parameter *ip*.

longer-prefixes —— Specify the destination subnets that match the network segment determined by the ip and mask parameters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the shortest route to 192.168.0.100:

Device(config)# show ip route specify 192.168.0.100

Look up the route entry with the destination as 192.168.0.0/24:

Device(config)# show ip route specify 192.168.0.0 255.255.255.0

Display the routes to all the subnets that belongs to 192.168.0.0/16:

Device(config)# show ip route specify 192.168.0.0 255.255.0.0 **longer-prefixes**

31.17 show ip route summary

Description

This **show ip route summary** command is used to display the summary information of the route entries classified by their sources.

Syntax

show ip route summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of route entries:

Device(config)# show ip route summary

31.18 show ipv6 interface

Description

This command is used to display the configured IPv6 information of the management interface, including ipv6 function status, link-local address and global address, IPv6 multicast groups etc.

Syntax

show ipv6 interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 information of the management interface:

Device(config)# show ipv6 interface

31.19 show ipv6 route

Description

This **show ipv6 route** command is used to display the IPv6 route entries of the specified type.

Syntax

show ipv6 route [static | connected]

Parameter

static | connected —— Specify the route type. If not specified, all types of route entries will be displayed.

static: The static routes.

connected: The connected routes.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 static routes:

Device(config)# show ipv6 route static

31.20 show ipv6 route summary

Description

This **show ipv6 route summary** command is used to display the summary information of the IPv6 route entries classified by their sources.

Syntax

show ipv6 route summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of IPv6 route entries:

```
Device(config)# show ipv6 route summary
```

Chapter 32 IPv6 Address Configuration Commands

The IPv6 address configuration commands are provided in the Interface Configuration Mode, which includes the routed port, the port-channel interface and the VLAN interface. Enter the configuration mode of these Layer 3 interfaces and configure their IPv6 parameters.

32.1 ipv6 enable

Description

This command is used to enable the IPv6 function on the specified Layer 3 interface. IPv6 function should be enabled before the IPv6 address configuration management. By default it is enabled on VLAN interface 1. IPv6 function can only be enabled on one Layer 3 interface at a time.

If the IPv6 function is disabled, the corresponding IPv6-based modules will be invalid, for example SSHv6, SSLv6, TFTPv6 and more. To disable the IPv6 function, please use **no ipv6 enable** command.

Syntax

ipv6 enable

no ipv6 enable

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IPv6 function on the VLAN interface 1:

```
Device(config)# interface vlan 1
Device(config-if)# ipv6 enable
```

32.2 ipv6 address autoconfig

Description

This command is used to enable the automatic configuration of the ipv6 link-local address. The device has only one ipv6 link-local address, which can be configured automatically or manually. The general ipv6 link-local address

has the prefix as fe80::/10. IPv6 routers cannot forward packets that have link-local source or destination addresses to other links. The autu-configured ipv6 link-local address is in EUI-64 format. To verify the uniqueness of the link-local address, the manually configured ipv6 link-local address will be deleted when the auto-configured ipv6 link-local address takes effect.

Syntax

ipv6 address autoconfig

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the automatic configuration of the ipv6 link-local address on VLAN interface 1:

Device(config)# interface vlan 1

Device(config-if)# ipv6 address autoconfig

32.3 ipv6 address link-local

Description

The **ipv6 address link-local** command is used to configure the ipv6 link-local address manually on a specified interface. To delete the configured link-local address, please use **no ipv6 address link-local** command.

Syntax

ipv6 address *ipv6-addr* **link-local**

no ipv6 address *ipv6-addr* **link-local**

Parameter

ipv6-addr —— The link-local address of the interface. It should be a standardized IPv6 address with the prefix fe80::/10, otherwise this command will be invalid.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the link-local address as fe80::1234 on the VLAN interface 1:

Device(config)# interface vlan 1

Device(config-if)# ipv6 address fe80::1234 **link-local**

32.4 ipv6 address dhcp

Description

The **ipv6 address dhcp** command is used to enable the DHCPv6 Client function. When this function is enabled, the Layer 3 interface will try to obtain IP from DHCPv6 server. To delete the allocated IP from DHCPv6 server and disable the DHCPv6 Client function, please use **no ipv6 address dhcp** command.

Syntax

ipv6 address dhcp

no ipv6 address dhcp

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Client function on VLAN interface 1:

Device(config)# interface vlan 1

Device(config-if)# ipv6 address dhcp

32.5 ipv6 address ra

Description

This command is used to configure the interface's global IPv6 address according to the address prefix and other configuration parameters from its

received RA(Router Advertisement) message. To disable this function, please use **no ipv6 address ra** command.

Syntax

ipv6 address ra

no ipv6 address ra

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the automatic ipv6 address configuration function to obtain IPv6 address through the RA message on VLAN interface 1:

Device(config)# interface vlan 1

Device(config-if)# ipv6 address ra

32.6 ipv6 address eui-64

Description

This command is used to manually configure a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits on the interface. Specify only the network prefix. The last 64 bits are automatically computed from the device MAC address. To remove a EUI-64 IPv6 address from the interface, please use the **no ipv6 address eui-64** command.

Syntax

ipv6 address *ipv6-addr* **eui-64**

no ipv6 address *ipv6-addr* **eui-64**

Parameter

ipv6-addr —— Global IPv6 address with 64 bits network prefix, for example 3ffe::/64.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure an EUI-64 global address on the interface with the network prefix 3ffe::/64:

```
Device(config)# interface vlan 1
Device(config-if)# ipv6 address 3ffe::/64 eui-64
```

32.7 ipv6 address

Description

This command is used to manually configure a global IPv6 address on the interface. To remove a global IPv6 address from the interface, please use **no ipv6 address** command.

Syntax

ipv6 address *ipv6-addr*

no ipv6 address *ipv6-addr*

Parameter

ipv6-addr —— Global IPv6 address with network prefix, for example 3ffe::1/64.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the global address 3001::1/64 on VLAN interface 1:

```
Device(config)# interface vlan 1
Device(config-if)# ipv6 address 3001::1/64
```

32.8 show ipv6 interface

Description

This command is used to display the configured ipv6 information of the management interface, including ipv6 function status, link-local address and global address, ipv6 multicast groups etc.

Syntax

show ipv6 interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ipv6 information of the management interface:

```
Device(config)# show ipv6 interface
```

Chapter 33 ARP Commands

Address Resolution Protocol (ARP) is used to resolve an IP address into an Ethernet MAC address. The device maintains an ARP mapping table to record the IP-to-MAC mapping relations, which is used for forwarding packets. An ARP mapping table contains two types of ARP entries: dynamic and static. An ARP dynamic entry is automatically created and maintained by ARP. A static ARP entry is manually configured and maintained.

33.1 arp

Description

This **arp** command is used to add a static ARP entry. To delete the specified ARP entry, please use the **no arp** command.

Syntax

arp *ip mac type*

no arp *ip type*

Parameter

ip —— The IP address of the static ARP entry.

mac —— The MAC address of the static ARP entry.

type —— The ARP type. Configure it as “arpa”.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a static ARP entry with the IP as 192.168.0.1 and the MAC as 00:11:22:33:44:55:

```
Device(config)# arp 192.168.0.1 00:11:22:33:44:55 arpa
```

33.2 clear arp-cache

Description

This **clear arp-cache** command is used to clear all the dynamic ARP entries.

Syntax

clear arp-cache

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear all the dynamic ARP entries:

```
Device(config)# clear arp-cache
```

33.3 arp dynamicrenew

Description

This **arp dynamicrenew** command is used to automatically renew dynamic ARP entries. To disable the device to automatically renew dynamic ARP entries, please use the **no arp dynamicremew** command. By default, it is enabled.

Syntax

arp dynamicremew

no arp dynamicremew

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the device to automatically renew the dynamic ARP entries:

```
Device(config)# arp dynamicrenew
```

33.4 arp timeout

Description

This **arp timeout** command is used to configure the ARP aging time of the interface.

Syntax

arp timeout *timeout*

no arp timeout

Parameter

timeout —— Specify the aging time, ranging from 10 to 3000 seconds. The default value is 1200 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ARP aging time as 60 seconds:

Device(config)# arp timeout 60

33.5 gratuitous-arp intf-status-up enable

Description

This **gratuitous-arp intf-status-up enable** command is used to enable the Layer 3 interface to send a gratuitous ARP packet when the interface's status becomes up.

Syntax

gratuitous-arp intf-status-up enable

no gratuitous-arp intf-status-up enable

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Enable the device's Layer 3 interfaces to send gratuitous ARP packets when their status becomes up:

```
Device(config)# gratuitous-arp intf-status-up enable
```

33.6 gratuitous-arp dup-ip-detected enable

Description

This **gratuitous-arp dup-ip-detected enable** command is used to enable the Layer 3 interface to send a gratuitous ARP packet when receiving a gratuitous packets of which the IP address is the same as its own.

Syntax

gratuitous-arp dup-ip-detected enable

no gratuitous-arp dup-ip-detected enable

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Enable the device's Layer 3 interface to send gratuitous ARP packets when receiving a gratuitous packets of which the IP address is the same as its own:

```
Device(config)# gratuitous-arp dup-ip-detected enable
```

33.7 gratuitous-arp learning enable

Description

This **gratuitous-arp learning enable** command is used to enable the Layer 3 interface to learn MAC addresses from the gratuitous ARP packets.

Syntax

gratuitous-arp learning enable

no gratuitous-arp learning enable

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Enable the Layer 3 interface to learn MAC addresses from the gratuitous ARP packets:

```
Device(config)# gratuitous-arp learning enable
```

33.8 gratuitous-arp send-interval

Description

This **gratuitous-arp send-interval** command is used to configure the interval at which the interface periodically send the gratuitous ARP packets.

Syntax

gratuitous-arp send-interval *interval*

Parameter

Interval —— Specify the interval at which the interface periodically send the gratuitous ARP packets. Value 0 means the interface will not send gratuitous ARP packets.

Command Mode

Interface Configuration Mode (interface vlan)

Privilege Requirement

None.

Example

Specify the interface VLAN 1 to send gratuitous ARP packets every 1 second:

```
Device(config)# interface vlan 1
Device(config-if)# gratuitous-arp send-interval 1
```

33.9 ip proxy-arp

Description

The **ip proxy-arp** command is used to enable Proxy ARP function on the specified VLAN interface or routed port. To disable Proxy ARP on this interface, please use **no ip proxy-arp** command.

Syntax

ip proxy-arp

no ip proxy-arp

Command Mode

Interface Configuration Mode (interface vlan)

Privilege Requirement

None

Example

Enable the Proxy ARP function on VLAN Interface 2:

```
Device(config)# interface vlan 2
Device(config-if)# ip proxy-arp
```

Enable the Proxy ARP function on routed port 1/0/2:

```
Device(config)# interface gigabitEthernet 2
Device(config-if)# no switchport
Device(config-if)# ip proxy-arp
```

33.10 ip local-proxy-arp

Description

The **ip local-proxy-arp** command is used to enable Local Proxy ARP function on the specified VLAN interface or routed port. To disable Local Proxy ARP function on this interface, please use **no ip local-proxy-arp** command.

Syntax

ip local-proxy-arp

no ip local-proxy-arp

Command Mode

Interface Configuration Mode (Interface vlan)

Privilege Requirement

None

Example

Enable the Proxy ARP function on VLAN Interface 2:

```
Device(config)# interface vlan 2
Device(config-if)# ip local-proxy-arp
```

Enable the Proxy ARP function on routed port 1/0/2:

```
Device(config)# interface gigabitEthernet 2
Device(config-if)# no switchport
Device(config-if)# ip local-proxy-arp
```

33.11 show arp

Description

This **show arp** command is used to display the active ARP entries. If no parameter is speicified, all the active ARP entries will be displayed.

Syntax

show arp [*ip*] [*mac*]

Parameter

ip —— Specify the IP address of your desired ARP entry.

mac —— Specify the MAC address of your desired ARP entry.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP entry with the IP as 192.168.0.2:

```
Device(config)# show arp 192.168.0.2
```

33.12 show ip arp (interface)

Description

This **show ip arp (interface)** command is used to display the active ARP entries associated with a specified Layer 3 interface.

Syntax

show ip arp { gigabitEthernet *port* | port-channel *port-channel-id* | vlan *id*}

Parameter

port —— Specify the number of the routed port.

port-channel-id —— Specify the ID of the port channel.

id —— Specify the VLAN interface ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP entry associated with VLAN interface 2:

```
Device(config)# show ip arp vlan 2
```

33.13 show ip arp summary

Description

This **show ip arp summary** command is used to display the number of the active ARP entries.

Syntax

show ip arp summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the number of the ARP entries:

Device(config)# show ip arp summary

33.14 show gratuitous-arp

Description

This **show gratuitous arp** command is used to display the configuration of gratuitous ARP.

Syntax

show gratuitous-arp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of gratuitous ARP:

Device(config)# show gratuitous-arp

33.15 show ip proxy-arp

Description

The **show ip proxy-arp** command is used to display the Proxy ARP status.

Syntax

show ip proxy-arp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Display the Proxy ARP status:

```
Device(config)# show ip proxy-arp
```

33.16 show ip local-proxy-arp

Description

The **show ip local-proxy-arp** command is used to display the Local Proxy ARP status.

Syntax

show ip local-proxy-arp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Display the Local Proxy ARP status:

```
Device(config)# show ip local-proxy-arp
```

Chapter 34 DHCP Server Commands

DHCP (Dynamic Host Configuration Protocol) is a network configuration protocol for hosts on TCP/IP networks, and it provides a framework for distributing configuration information to hosts. DHCP server assigns IP addresses from specified address pools to DHCP clients and manages them.

34.1 service dhcp server

Description

The **service dhcp server** command is used to enable DHCP service globally. To disable DHCP server service, please use **no service dhcp server** command.

Syntax

service dhcp server

no service dhcp server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP server service globally:

```
Device(config)# service dhcp server
```

34.2 ip dhcp server extend-option capwap-ac-ip

Description

The **ip dhcp server extend-option capwap-ac-ip** command is used to specify the Option 138, which should be configured as the management IP address of an AC (Access Control) device. If the APs in the local network request this option, the server will inform the APs of the AC's IP address by sending a packet containing this option. To delete the Option 138, please use **no ip dhcp server extend-option capwap-ac-ip** command.

Syntax

ip dhcp server extend-option capwap-ac-ip *ip-address*

no ip dhcp server extend-option capwap-ac-ip

Parameter

ip-address —— Specify the management IP address of an AC (Access Control) device.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the remote DHCP server's IP address as 192.168.3.1:

Device(config)# ip dhcp server extend-option capwap-ac-ip 192.168.3.1

34.3 ip dhcp server extend-option vendor-class-id

Description

The **ip dhcp server extend-option vendor-class-id** command is used to configure the class ID of the packets from DHCP server in a different network segment. To delete the class ID settings, please use **no ip dhcp server extend-option vendor-class-id** command.

Syntax

ip dhcp server extend-option vendor-class-id *class-id*

no ip dhcp server extend-option vendor-class-id

Parameter

class-id —— Specify the class ID of the DHCP packets from another network segment.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the class ID of the DHCP packets from another network segment as 34:

Device(config)# ip dhcp server extend-option vendor-class-id 34

34.4 ip dhcp server exclude-address

Description

The **ip dhcp server exclude-address** command is used to specify the reserved IP addresses which are forbidden to allocate, such as the gateway address, the network segment broadcast address, the server address etc. To delete the reserved IP addresses, please use **no ip dhcp server exclude-address** command.

Syntax

ip dhcp server exclude-address *start-ip-address end-ip-address*

no ip dhcp server exclude-address *start-ip-addr end-ip-address*

Parameter

start-ip-address —— Specify the start IP address of the reserved IP pool.

end-ip-address —— Specify the end IP address of the reserved IP pool. Only one IP address will be reserved if the end IP address and the start IP address are the same.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the reserved IP addresses from 192.168.1.1 to 192.168.1.9:

Device(config)# ip dhcp server exclude-address 192.168.1.1 192.168.1.9

34.5 ip dhcp server pool

Description

The **ip dhcp server pool** command is used to create the address pool of DHCP Server and enter the dhcp configuration mode. To delete the address pool, please use **no ip dhcp server pool** command.

Syntax

ip dhcp server pool *pool-name*

no ip dhcp server pool *pool-name*

Parameter

pool-name —— Specify the address pool name, ranging from 1 to 8 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create the address pool of name POOL1:

```
Device(config)# ip dhcp server pool POOL1
```

34.6 ip dhcp server ping timeout

Description

The **ip dhcp server ping timeout** command is used to specify the timeout of PING process. To resume the default value, please use **no ip dhcp server ping timeout** command.

Syntax

ip dhcp server ping timeout *value*

no ip dhcp server ping timeout

Parameter

value —— Specify the timeout value, ranging from 100 to 10000ms. The default value is 100ms.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the timeout of PING as 200ms:

```
Device(config)# ip dhcp server ping timeout 200
```

34.7 ip dhcp server ping packets

Description

The **ip dhcp server ping packets** command is used to specify the number of PING packets sent. If this value is set to 0, the PING process will be disabled. To resume the default value, please use **no ip dhcp server ping packets** command.

Syntax

ip dhcp server ping packets *num*

Parameter

num —— Specify the PING packets' number, ranging from 0 to 10. By default it's 1.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the PING packets' number as 2:

```
Device(config)# ip dhcp server ping packets 2
```

34.8 network

Description

The **network** command is used to specify the address and subnet of the network pool.

Syntax

network *network-address subnet-mask*

Parameter

network-address —— Specify the network address of the pool, with the format A.B.C.D. All the IP addresses in the same subnet are allocatable except the reserved addresses and specific addresses.

subnet-mask —— Specify the subnet mask of the pool, with the format A.B.C.D.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool "product" as 192.168.1.0 255.255.255.0:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# network 192.168.1.0 255.255.255.0

34.9 lease

Description

The **lease** command is used to specify the lease time of the address pool.

Syntax

lease *lease-time*

Parameter

lease-time —— Specify the lease time of the pool, ranging from 1 to 2880 minutes. The default value is 120 minutes.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the lease time of address pool "product" as 10 minutes:

Device(config)# ip dhcp server pool product

```
Device(dhcp-config)# lease 10
```

34.10 address hardware-address

Description

The **address hardware-address** command is used to reserve the static address bound with hardware address in the address pool. To delete the binding, please use **no address hardware-address**.

Syntax

address *ip-address* **hardware-address** *hardware-address* **hardware-type** { ethernet | ieee802 }

no address *ip-address*

Parameter

ip-address —— Specify the static binding IP address.

hardware-address —— Specify the hardware address, in the format XX:XX:XX:XX:XX:XX.

ethernet | ieee802 —— Specify the hardware type.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Reserve the IP address 192.168.0.10 in the address pool "product" for the device with the MAC address as 5e:4c:a6:31:24:01 and the hardware type as ethernet:

```
Device(config)# ip dhcp server pool product

Device(dhcp-config)# address 192.168.0.10 hardware-address

5e:4c:a6:31:24:01 hardware-type ethernet
```

34.11 address client-identifier

Description

The **address client-identifier** command is used to specify the static address bound with client ID in the address pool. To delete the binding, please use **no address** command.

Syntax

address *ip-address* **client-identifier** *client-id* [ascii]

no address *ip-address*

Parameter

ip-address —— Specify the static binding IP address.

client-id —— Specify the client ID, in the format of hex value.

ascii —— The client ID is entered with ASCII characters.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Reserve the IP address 192.168.0.10 in the address pool "product" for the device with the client ID as abc in ASCII:

Device(config)# ip dhcp pool product

Device(dhcp-config)# address 192.168.0.10 **client-identifier** abc **ascii**

34.12 default-gateway

Description

The **default-gateway** command is used to specify the default gateway of the address pool. To delete the configuration, please use **no default-gateway**.

Syntax

default-gateway *gateway-list*

no default-gateway

Parameter

gateway-list —— Specify the gateway list, with the format of A.B.C.D,E.F.G.H. At most 8 gateways can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool product's default gateways as 192.168.0.1 and 192.168.1.1:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# default-gateway 192.168.0.1,192.168.1.1

34.13 dns-server

Description

The **dns-server** command is used to specify the DNS server of the address pool. To delete this configuration, please use **no dns-server** command.

Syntax

dns-server *dns-list*

no dns-server

Parameter

dns-list —— Specify the DNS server list, with the format of A.B.C.D,E.F.G.H. At most 8 DNS servers can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool's DNS servers as 192.168.0.1 and 192.168.1.1:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# dns-server 192.168.0.1,192.168.1.1

34.14 netbios-name-server

Description

The **netbios-name-server** command is used to specify the Netbios server's IP address. To delete the Netbios servers, please use **no netbios-name-server** command.

Syntax

netbios-name-server *NBNS-list*

no netbios-name-server

Parameter

NBNS-list —— Specify the Netbios server list, with the format of A.B.C.D,E.F.G.H. At most 8 Netbios servers can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool's Netbios servers as 192.168.0.1 and 192.168.1.1:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# netbios-name-server 192.168.0.1,192.168.1.1

34.15 netbios-node-type

Description

The **netbios-node-type** command is used to specify the Netbios server's node type. To delete the node type setttings, please use **no netbios-node-type** command.

Syntax

netbios-node-type *type*

no netbios-node-type

Parameter

type —— Specify the node type as b-node, h-node, m-node or p-node.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the address pool's Netbios server type as b-node:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# netbios-node-type b-node

34.16 next-server

Description

The **next-server** command is used to specify the next DHCP server's address during the DHCP boot process. To delete the next server, please use **no next-server** command.

Syntax

next-server *ip-address*

next-server

Parameter

ip-address —— Specify the IP address of the next server.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the next server's IP address as 192.168.2.1:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# next-server 192.168.2.1

34.17 domain-name

Description

The **domain-name** command is used to specify the domain name for the DHCP client. To delete the domain name, please use **no domain-name** command.

Syntax

domain-name *domainname*

no domain-name

Parameter

domainname —— Specify the domain name for the DHCP client.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the DHCP client's domain name as edu:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# domain-name edu

34.18 bootfile

Description

The **bootfile**command is used to specify the name of the DHCP client's bootfile. To delete the bootfile, please use **no bootfile** command.

Syntax

bootfile *file-name*

no bootfile

Parameter

file-name —— Specify the name of the DHCP client's bootfile.

Command Mode

DHCP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the name of the DHCP client's bootfile as boot1:

Device(config)# ip dhcp server pool product

Device(dhcp-config)# bootfile boot1

34.19 show ip dhcp server status

Description

The **show ip dhcp server status** command is used to display the status of the DHCP service.

Syntax

show ip dhcp server status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the status of DHCP service:

Device(config)# show ip dhcp server status

34.20 show ip dhcp server statistics

Description

The **show ip dhcp server statistics** command is used to display the DHCP packets received and sent by DHCP server.

Syntax

show ip dhcp server statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics of DHCP packets received and sent by the DHCP server:

```
Device(config)# show ip dhcp server statistics
```

34.21 show ip dhcp server extend-option

Description

The **show ip dhcp server extend-option** command is used to display the configuration of the remote DCHP servers.

Syntax

show ip dhcp server extend-option

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of the remote DCHP servers:

```
Device(config)# show ip dhcp server extend-option
```

34.22 show ip dhcp server pool

Description

The **show ip dhcp server pool** command is used to display the configuration of the address pool.

Syntax

show ip dhcp server pool

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured address pool:

```
Device(config)# show ip dhcp server pool
```

34.23 show ip dhcp server excluded-address

Description

The **show ip dhcp server excluded-address** command is used to display the configuration of reserved addresses.

Syntax

show ip dhcp server excluded-address

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured reserved addresses:

```
Device(config)# show ip dhcp server excluded-address
```

34.24 show ip dhcp server manual-binding

Description

The **show ip dhcp server manual-binding** command is used to display the configuration of static binding address.

Syntax

show ip dhcp server manual-binding

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured static binding address:

```
Device(config)# show ip dhcp server manual-binding
```

34.25 show ip dhcp server binding

Description

The **show ip dhcp server binding** command is used to display the binding entries.

Syntax

show ip dhcp server binding [ip *ip-address*]

Parameter

ip-address —— Specify the binding IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the address binding entries:

```
Device(config)# show ip dhcp server binding
```

34.26 clear ip dhcp server statistics

Description

The **clear ip dhcp server statistics** command is used to clear the statistics information of DHCP packets.

Syntax

clear ip dhcp server statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the packet statistics:

```
Device(config)# clear ip dhcp server statistics
```

34.27 clear ip dhcp server binding

Description

The **clear ip dhcp server binding** command is used to clear the binding information.

Syntax

clear ip dhcp server binding [*ip-address*]

Parameter

ip-address —— Specify the binding IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear all the binding addresses:

```
Device(config)# clear ip dhcp server binding
```

Chapter 35 DHCP Relay Commands

A DHCP Relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. DHCP Relay forward requests and replies between clients and servers when they are not on the same physical subnet.

35.1 service dhcp relay

Description

The **service dhcp relay** command is used to enable DHCP Relay function globally. To disable DHCP Relay function, please use **no service dhcp relay** command.

Syntax

service dhcp relay

no service dhcp relay

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP Relay function globally:

```
Device(config)# service dhcp relay
```

35.2 ip dhcp relay hops

Description

The **ip dhcp relay hops** command is used to specify the maximum hops (DHCP Relay agent) that the DHCP packets can be relayed. To restore the default value, please use **no service dhcp relay hops** command.

Syntax

ip dhcp relay hops *hops*

no ip dhcp relay hops

Parameter

hops——Specify the maximum hops (DHCP Relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped. The valid value ranges from the 1 to 16, and the default value is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of relay hops as 6:

Device(config)# ip dhcp relay hops 6

35.3 ip dhcp relay time

Description

The **ip dhcp relay time** command is used to specify the DHCP relay time threshold. DHCP relay time is the time elapsed since client began address acquisition or renewal process. When the elapsed time of the DHCP packet is greater than the value set here, the DHCP packet will be dropped by the device. To restore the default value, please use **no service dhcp relay time** command.

Syntax

ip dhcp relay time *time*

no ip dhcp relay time

Parameter

time——Specify the DHCP relay time threshold. The valid value ranges from 1 to 65535. The default value is 0, which means the device will not examine this field of the DHCP packets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the DHCP Relay time as 30 seconds:

```
Device(config)# ip dhcp relay time 30
```

35.4 ip helper-address

Description

The **ip helper-address** command is used to add DHCP Server address to the Layer 3 interface. To delete the server address, please use **no ip helper-address** command.

Syntax

ip helper-address *ip-address*

no ip helper-address [*ip-address*]

Parameter

ip-address —— DHCP Server address.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add DHCP Server address 192.168.2.1 to interface VLAN 1:

```
Device(config)# interface vlan 1

Device(config-if)# ip helper-address 192.168.2.1
```

35.5 ip dhcp relay dynamic-circuit-id

Description

The **ip dhcp relay dynamic-circuit-id** command is used to configure the dynamic Circuit ID for DHCP Option 82. The dynamic Circuit ID consists of up to 5 parameters. To restore the dynamic Circuit ID configuration to the default, use the **no ip dhcp relay dynamic-circuit-id** command.

Syntax

ip dhcp relay dynamic-circuit-id param1 param2 param3 param4 param5 format1 format2 format3 format4 format5 custom-string *string*

no ip dhcp relay dynamic-circuit-id

Parameter

param1 - param5 —— Component parameters of the dynamic Circuit ID. Valid values:

none —— None (placeholder, no content is filled)

pon-id —— PON port ID

onu-id —— ONU ID

olt-mac —— OLT MAC address

onu-sn —— ONU serial number

onu-mac —— ONU MAC address

onu-port —— ONU port number

subscriber-id —— Subscriber ID

system-id —— System ID

slot-id —— Slot ID

vlan-id —— VLAN ID

custom —— Custom string

format1 - format5 —— Encoding format for the corresponding param1 - param5. Valid values:

char —— ASCII format (default)

hex —— Hexadecimal format

Note: olt-mac, onu-sn, onu-mac, and custom types only support ASCII format and do not support hex format.

custom-string string —— When the custom type is selected for a parameter, specifies the custom string content, up to 125 characters. The custom type can only appear once.

Usage Guideline

At least one parameter must be set to a value other than none. Setting all parameters to none is not allowed.

Duplicate component types are not allowed.

The custom type can only be specified once. When custom is selected, the custom-string must be provided and cannot be empty.

olt-mac, onu-sn, onu-mac, and custom parameters only support char (ASCII) format. Setting them to hex will result in an error.

Example

Configure the dynamic Circuit ID composed of PON-ID, ONU-ID, and VLAN-ID:

(config)# ip dhcp relay dynamic-circuit-id param1 pon-id param2 onu-id param3 vlan-id

Configure the dynamic Circuit ID composed of PON-ID (ASCII format) and VLAN-ID (hex format):

(config)# ip dhcp relay dynamic-circuit-id param1 pon-id param2 vlan-id format2 hex

Configure the dynamic Circuit ID with a custom string "TP-Link":

(config)# ip dhcp relay dynamic-circuit-id param1 pon-id param2 param2 custom custom_string "TPLINK"

35.6 ip dhcp relay dynamic-remote-id

Description

The **ip dhcp relay dynamic-remote-id** command is used to configure the dynamic remote ID for DHCP Option 82. The dynamic remote ID consists of up to 5 parameters. To restore the dynamic remote ID configuration to the default, use the **no ip dhcp relay dynamic- remote -id** command.

Syntax

ip dhcp relay dynamic-remote-id param1 param2 param3 param4 param5 format1 format2 format3 format4 format5 custom-string *string*

no ip dhcp relay dynamic-remote-id

Parameter

param1 - param5 —— Component parameters of the dynamic Circuit ID. Valid values:

none —— None (placeholder, no content is filled)

pon-id —— PON port ID

onu-id —— ONU ID

olt-mac —— OLT MAC address

onu-sn —— ONU serial number

onu-mac —— ONU MAC address

onu-port —— ONU port number

subscriber-id —— Subscriber ID

system-id —— System ID

slot-id —— Slot ID

vlan-id —— VLAN ID

custom —— Custom string

format1 - format5 —— Encoding format for the corresponding param1 - param5. Valid values:

char —— ASCII format (default)

hex —— Hexadecimal format

Note: olt-mac, onu-sn, onu-mac, and custom types only support ASCII format and do not support hex format.

custom-string string —— When the custom type is selected for a parameter, specifies the custom string content, up to 125 characters. The custom type can only appear once.

Usage Guideline

At least one parameter must be set to a value other than none. Setting all parameters to none is not allowed.

Duplicate component types are not allowed.

The custom type can only be specified once. When custom is selected, the custom-string must be provided and cannot be empty.

olt-mac, onu-sn, onu-mac, and custom parameters only support char (ASCII) format. Setting them to hex will result in an error.

Example

Configure the dynamic Circuit ID composed of PON-ID, ONU-ID, and VLAN-ID:

(config)# ip dhcp relay dynamic-remote-id param1 pon-id param2 onu-id param3 vlan-id

Configure the dynamic Circuit ID composed of PON-ID (ASCII format) and VLAN-ID (hex format):

(config)# ip dhcp relay dynamic-remote-id param1 pon-id param2 vlan-id format2 hex

Configure the dynamic Circuit ID with a custom string "TP-Link":

(config)# ip dhcp relay dynamic-remote-id param1 pon-id param2 param2 custom custom_string "TPLINK"

35.7 ip dhcp relay information option

Description

The **ip dhcp relay information option** command is used to enable option 82 support in DHCP Relay. To disable this function, please use **no ip dhcp relay information option** command.

Syntax

ip dhcp relay information option

no ip dhcp relay information option

Command Mode

Interface Configuration Mode (interface gigabitEthernet/interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option 82 support in DHCP Relay for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp relay information option

35.8 ip dhcp relay information strategy

Description

The **ip dhcp relay information strategy** command is used to specify the operation for the Option 82 field of the DHCP request packets from the Host. To restore to the default option, please use **no ip dhcp relay information strategy** command.

Syntax

ip dhcp relay information strategy { drop | keep | replace }

no ip dhcp relay information strategy

Parameter

drop | keep | replace ——The operations for Option 82 field of the DHCP request packets from the Host. The default operation is keep.

drop: Discard the packet with the Option 82 field.

keep: Keep the Option 82 field in the packet.

replace: Replace the option 82 field with the system option defined by the switch.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the option 82 strategy as replace to replace the Option 82 field with the local parameter on receiving the DHCP request packet for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp relay information strategy replace

35.9 ip dhcp relay information format

Description

The **ip dhcp relay information format** command is used to select the format of option 82 sub-option value field. To restore to the default option, please use **no ip dhcp relay information format** command.

Syntax

ip dhcp relay information format { normal | private }

no ip dhcp relay information format

Parameter

normal | private —— The format type of option 82 sub-option value field.

normal: Indicates that the format of sub-option value field is TLV (type-length-value).

private: Indicates that the format of sub-option value field is the value you

configure for the related sub-option.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Select the format of option 82 sub-option value field as TLV (type-length-value) for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)#ip dhcp relay information format normal

35.10 ip dhcp relay information circuit-id

Description

The **ip dhcp relay information circuit-id** command is used to specify the custom circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp relay information circuit-id** command.

Syntax

ip dhcp relay information circuit-id *circuitID*

no ip dhcp relay information circuit-id

Parameter

circuitID —— Specify the circuit ID, ranging from 1 to 64 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the circuit ID as “TP-Link” for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp relay information circuit-id TP-Link

35.11 ip dhcp relay information remote-id

Description

The **ip dhcp relay information remote-id** command is used to specify the custom remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp relay information remote-id** command.

Syntax

ip dhcp relay information remote-id *remoteID*

no ip dhcp relay information remote-id

Parameter

remoteID —— Specify the remote ID, ranging from 1 to 64 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the remote ID as “TP-Link” for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp relay information remote-id TP-Link

35.12 ip dhcp relay information circuit-id-dynamic

Description

The **ip dhcp relay information circuit-id-dynamic** command is used to specify a dynamic circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp relay information**

circuit-id-dynamic command. The circuit-id-dynamic command can only be configured on PON port series (gpon, xgspon).

Syntax

ip dhcp relay information circuit-id-dynamic

no ip dhcp relay information circuit-id-dynamic

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify port 2 to dynamic circuit ID:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp relay information circuit-id dynamic

35.13 ip dhcp relay information remote-id-dynamic

Description

The **ip dhcp relay information remote-id-dynamic** command is used to specify a dynamic remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp relay information remote-id-dynamic** command. The remote-id-dynamic command can only be configured on PON port series (gpon, xgspon).

Syntax

ip dhcp relay information remote-id-dynamic

no ip dhcp relay information remote-id-dynamic

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify port 2 to dynamic remote ID:

```
Device(config)#interface gigabitEthernet 1/0/2
Device(config-if)# ip dhcp relay information remote-id-dynamic
```

35.14 ip dhcp relay default-interface

Description

The **ip dhcp relay default-interface** command is used to configure default relay agent interface. When the device works at DHCP VLAN Relay mode and there is no IP interface in the VLAN, the device uses the IP of default relay agent interface to fill in the relay agent IP address field of DHCP packets. To delete the default relay agent interface use **no ip dhcp relay default-interface.**

Syntax

ip dhcp relay default-interface

no ip dhcp relay default-interface

Command mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure interface VLAN 1 as the default relay agent interface:

```
Device(config)# interface vlan 1
Device(config-if)# ip dhcp relay default-interface
```

35.15 ip dhcp relay vlan

Description

The **ip dhcp relay vlan** command is used to add DHCP server address to specified VLAN. If there is an IP interface in the VLAN and it has configured a DHCP server address at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets. To delete the DHCP server address use **no ip dhcp relay vlan.**

Syntax

ip dhcp relay vlan *vid* **helper-address** *ip-address*

no ip dhcp relay vlan *vid* **helper-address** *[ip-address]*

Parameter

vid—— VLAN ID.

ip-address—— DHCP Server address.

Command mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add DHCP server address 192.168.2.1 to VLAN 1:

```
Device(config)# ip dhcp relay vlan 1 helper-address 192.168.2.1
```

35.16 show ip dhcp relay

Description

The **show ip dhcp relay** command is used to display the global status and Option 82 configuration of DHCP Relay.

Syntax

show ip dhcp relay [[information interface] [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id* | gpon port]]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

Device(config)# show ip dhcp relay

35.17 show ip dhcp relay dynamic-option82

Description

The **show ip dhcp relay dynamic-option82** command is used to display the global dynamic status and Option 82 configuration of DHCP L2Relay.

Syntax

show ip dhcp relay dynamic-option82 [<cr>|circuit-id|remote-id]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the Option 82 dynamic remode-id configuration of the current DHCP relay:

Device# show ip dhcp relay dynamic-option82 remote-id

35.18 show ip dhcp relay information interface

Description

The **show ip dhcp relay information interface** command is used to display the all ports' cfg of Option 82 configuration of DHCP Relay.

Syntax

show ip dhcp relay dynamic-option82 [[information interface] [fastEthernet *port*| gigabitEthernet *port*| ten-gigabitEthernet *port*| port-channel *port-channel-id*| gpon port]]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

```
Device(config)# show ip dhcp relay
```

Chapter 36 DHCP L2 Relay Commands

36.1 ip dhcp l2relay

Description

The **ip dhcp l2relay** command is used to enable DHCP L2 Relay function globally. To disable DHCP L2 Relay function, please use **no ip dhcp l2relay** command.

Syntax

ip dhcp l2relay

no ip dhcp l2relay

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP L2 Relay function globally:

```
Device(config)# ip dhcp l2relay
```

36.2 ip dhcp l2relay vlan

Description

The **ip dhcp l2relay vlan** command is used to enable DHCP L2 relay in the specified VLAN. To disable DHCP L2 Relay in the specific vlan, please use **no ip dhcp l2relay vlan** command.

Syntax

ip dhcp l2relay vlan *vlan-range*

no ip dhcp l2relay vlan *vlan-range*

Parameter

vlan-range —— Specify the vlan to be enabled with DHCP L2 relay.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP L2 Relay for VLAN 2:

Device(config)# ip dhcp l2relay vlan 2

36.3 ip dhcp l2relay dynamic-circuit-id

Description

The **ip dhcp l2relay dynamic-circuit-id** command is used to configure the format of dhcp option 82. There are five types of data that can be filled in: pon-id/onu-id/onu-sn/olt-mac/onu-mac. You can also fill in none, in which case the parameter will be skipped.

Syntax

ip dhcp l2relay dynamic-circuit-id {param1 {*param*} param2 {*param*} param3 {*param*} param4 {*param*} param5 {*param*} }

Parameter

param —— The parameter name. Enumeration variable. You can select any parameter to fill in, but not all parameters can be left blank. You must fill in one of pon-id/onu-id/onu-sn/olt-mac/onu-mac/none, otherwise an error will be reported.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the format of dhcp option 82:

Device(config)# ip dhcp l2relay dynamic-circuit-id param1 onu-id

36.4 ip dhcp l2relay dynamic-remote-id

Description

The **ip dhcp l2relay dynamic-remote-id** command is used to configure the format of dhcp option 82 remote id. There are five types of data that can be

filled in: pon-id/onu-id/onu-sn/olt-mac/onu-mac. You can also fill in none, in which case the parameter will be skipped.

Syntax

ip dhcp l2relay dynamic-remote-id {param1 {*param*} param2 {*param*} param3 {*param*} param4 {*param*} param5 {*param*} }

Parameter

param —— The parameter name. Enumeration variable. You can select any parameter to fill in, but not all parameters can be left blank. You must fill in one of pon-id/onu-id/onu-sn/olt-mac/onu-mac/none, otherwise an error will be reported.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the format of dhcp option 82 remote id:

Device(config)# ip dhcp l2relay dynamic-remote-id param1 onu-id

36.5 ip dhcp l2relay information option

Description

The **ip dhcp l2relay information option** command is used to enable option 82 support in DHCP Relay. To disable this function, please use **no ip dhcp l2relay information option** command.

Syntax

ip dhcp l2relay information option

no ip dhcp l2relay information option

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable option 82 support in DHCP Relay for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp l2relay information option

36.6 ip dhcp l2relay information strategy

Description

The **ip dhcp l2relay information strategy** command is used to specify the operation for the Option 82 field of the DHCP request packets from the Host. To restore to the default option, please use **no ip dhcp l2relay information strategy** command.

Syntax

ip dhcp l2relay information strategy { drop | keep | replace }

no ip dhcp l2relay information strategy

Parameter

drop | keep | replace —— The operations for Option 82 field of the DHCP request packets from the Host. The default operation is keep.

drop: Discard the packet with the Option 82 field.

keep: Keep the Option 82 field in the packet.

replace: Replace the option 82 field with the system option defined by the device.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the option 82 strategy as replace to replace the Option 82 field with the local parameter on receiving the DHCP request packet for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp l2relay information strategy replace

36.7 ip dhcp l2relay information format

Description

The **ip dhcp l2relay information format** command is used to select the format of option 82 sub-option value field. To restore to the default option, please use **no ip dhcp l2relay information format** command.

Syntax

ip dhcp l2relay information format { normal | private }

no ip dhcp l2relay information format

Parameter

normal | private —— The format type of option 82 sub-option value field.

normal: Indicates that the format of sub-option value field is TLV (type-length-value).

private: Indicates that the format of sub-option value field is the value you configure for the related sub-option.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Select the format of option 82 sub-option value field as TLV (type-length-value) for port 2:

```
Device(config)#interface gigabitEthernet 1/0/2
Device(config-if)#ip dhcp l2relay information format normal
```

36.8 ip dhcp l2relay information circuit-id

Description

The **ip dhcp l2relay information circuit-id** command is used to specify the custom circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp l2relay information circuit-id** command.

Syntax

ip dhcp l2relay information circuit-id *circuitID*

no ip dhcp l2relay information circuit-id

Parameter

circuitID —— Specify the circuit ID, ranging from 1 to 64 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the circuit ID as "TP-Link" for port 2:

```
Device(config)#interface gigabitEthernet 1/0/2
Device(config-if)# ip dhcp l2relay information circuit-id TP-Link
```

36.9 ip dhcp l2relay information remote-id

Description

The **ip dhcp l2relay information remote-id** command is used to specify the custom remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp l2relay information remote-id** command.

Syntax

ip dhcp l2relay information remote-id *remoteID*

no ip dhcp l2relay information remote-id

Parameter

remoteID —— Specify the remote ID, ranging from 1 to 64 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the remote ID as "TP-Link" for port 2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)# ip dhcp l2relay information remote-id TP-Link

36.10 show ip dhcp l2relay

Description

The **show ip dhcp l2relay** command is used to display the global status and Option 82 configuration of DHCP Relay.

Syntax

show ip dhcp l2relay

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

Device(config)# show ip dhcp l2relay

36.11 show ip dhcp l2relay interface

Description

The **show ip dhcp l2relay interface** command is used to display the DHCP L2 Relay status for the ports.

Syntax

show ip dhcp l2relay interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id* | gpon port]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP L2 Relay configuration of port 1/0/2:

Device(config)# show ip dhcp l2relay interface gigabitEthernet 1/0/2

36.12 show ip dhcp l2relay dynamic-option82

Description

The **show ip dhcp l2relay dynamic-option82** command is used to display the dynamic Option 82 configuration of the current DHCP l2relay.

Syntax

show ip dhcp l2relay dynamic-option82 [<cr>|circuit-id|remote-id]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display the dynamic Option 82 remode id configuration of the current DHCP l2relay:

Device# show ip dhcp l2relay dynamic-option82 remote-id

36.13 show ip dhcp l2relay information interface

Description

The **show ip dhcp relay information interface** command is used to display the all ports' cfg of Option 82 configuration of DHCP Relay.

Syntax

show ip dhcp relay dynamic-option82 [[information interface] [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id* | gpon port]]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

```
Device(config)# show ip dhcp relay
```

Chapter 37 QoS Commands

QoS (Quality of Service) function is used to optimize the network performance. It provides you with network service experience of a better quality. The device implements three priority modes based on port, on 802.1p and on DSCP.

37.1 qos trust

Description

The **qos trust** command is used to configure the trust mode of CoS (Class of Service) function for the ports. The default trust mode is trust port priority.

Syntax

qos trust mode { dot1p | dscp}

Parameter

dot1p—— Trust 802.1p mode. In this mode, data will be classified into different services based on the 802.1p priority.

dscp—— Trust dscp mode. In this mode, data will be classified into different services based on the dscp priority.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the trust mode of port 1/0/3 as dscp:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# qos trust dscp
```

37.2 qos port-priority

Description

The **qos port-priority** command is used to configure the port to 802.1p priority mapping for the desired port. To return to the default configuration,

please use **no qos port-priority** command. When Port Priority is enabled, the packets will be mapped to different priority queues based on the ingress ports.

Syntax

qos port-priority { *dot1p-priority* }

no qos port-priority

Parameter

dot1p-priority —— The 802.1p priority that the packets will be mapped to from the desired port. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively. By default, the priority is 0.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the priority of port 5 as 3:

```
Device(config)# interface gigabitEthernet 1/0/5
Device(config-if)# qos port-priority 3
```

37.3 qos cos-map

Description

The **qos cos-map** command is used to configure 802.1p to queue mapping globally. To return to the default configuration, please use **no qos cos-map** command. When 802.1P Priority is enabled, the packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority.

Syntax

qos cos-map { *dot1p-priority* } { *tc-queue* }

no qos cos-map

Parameter

dot1p-priority —— The value of 802.1p priority. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively.

tc-queue—— The number of TC queue that the 80.1p priority will be mapped

to. It ranges from 0 to 7.

Command Mode

Interface Configuration Mode (interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Map the 802.1p priority 5 to TC-2:

```
Device (config)# qos cos-map 5 2
```

37.4 qos dot1p-remap

Description

The **qos dot1p-remap** command is used to configure the 802.1p to 802.1p mappings. To return to the default configuration, please use **no qos dot1p-remap** command. When 802.1p remap is configured, the packets with the specific 802.1p priority will tagged with the desired new 802.1p priority.

Syntax

qos dot1p-remap { *dot1p-priority*} { *new-dot1p-priority*}

no qos dot1p-remap

Parameter

dot1p-priority—— The original 802.1p priority. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively.

new-dot1p-priority—— The new 802.1p priority. It ranges from 0 to 7.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Remap 802.1p priority 5 to 802.1p priority 6:

```
Device(config)#qos dot1p-remap 5 6
```

For other devices:

Remap 802.1p priority 5 to 802.1p priority 6 for port 1/0/1:

```
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)#qos dot1p-remap 5 6
```

37.5 qos dscp-map

Description

The **qos dscp-map** command is used to configure the DSCP to 802.1p mapping. To return to the default configuration, please use **no qos dscp-map** command. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP Priority is enabled, IP datagram are mapped to different priority levels based on DSCP priority.

Syntax

qos dscp-map { *dscp-value-list* } { *dot1p-priority* }

no qos dscp-map

Parameter

dscp-value-list —— The DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63.

dot1p-priority ——The 802.1p priority to which the DSCP priority will be mapped. It ranges from 0 to 7, which represent 802.1p priority 0–7 respectively. By default, the priority is 0.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Map DSCP Priority 5 to 802.1p priority 2:

```
Device(config)#qos dscp-map 5 2
```

For other devices:

Map DSCP Priority 5 to 802.1p priority 2 for port 1/0/1:

```
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)#qos dscp-map 5 2
```

37.6 qos dscp-remap

Description

The **qos dscp-remap** command is used to configure the DSCP to DSCP mappings. To return to the default configuration, please use **no qos dscp-remap** command. When DSCP remap is configured, the packets with the specific DSCP priority will be changed to the desired new DSCP priority.

Syntax

qos queue dscp-map { *dscp-value-list* } { *dscp-remap-value* }

no qos queue dscp-map

Parameter

Dscp-value-list——The original DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63.

Dscp-remap-value—— The new DSCP value, which ranges from 0 to 63.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Map DSCP values 10-12 to DSCP value 2:

Device(config)# qos dscp-remap 10-12 2

For other devices:

Map DSCP values 10-12 to DSCP value 2 for port 1/0/2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# qos dscp-remap 10-12 2

37.7 qos queue mode

Description

The **qos queue mode** command is used to configure the Scheduler Mode. When the network is congested, the program that many packets complete for resources must be solved, usually in the way of queue scheduling. The device will control the forwarding sequence of the packets according to the priority queues and scheduling algorithms you set. On this device, the priority levels are labeled as TC0, TC1, TC2 ... TC7.

Syntax

qos queue { *tc-queue* } **mode** { sp | wrr } [weight *weight*]

Parameter

tc-queue —— The egress queue ID. It ranges from 0 to 7, which represents TC queue from TC0 to TC7 respectively.

sp —— Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr —— Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. If you select this mode, you need to specify the queue weight at the same time.

weight —— Configure the weight value of the specified TC queue. When the scheduler mode is specified as WRR, the weight value ranges from 1 to 127. The 8 queues will take up the bandwidth according to their ratio.

Command Mode

For some devices:

Global Configuration Mode

For other devices:

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

For some devices:

Specify the Scheduler Mode of TC1 as WRR and set the queue weight as 10:

```
Device(config)# qos queue 1 mode wrr weight 10
```

For other devices:

Specify the Scheduler Mode of TC1 as WRR and set the queue weight as 10 for port 1/0/1:

```
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# qos queue 1 mode wrr weight 10
```

37.8 show qos cos-map

Description

The **show qos cos-msp** command is used to display the 802.1p priority to TC queue mappings.

Syntax

show qos cos-map

show qos cos-map interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the 802.1p to queue mappings:

```
Device# show qos cos-map
```

37.9 show qos dot1p-remap interface

Note: This command is only available on certain devices.

Description

The **show qos dot1p-remap interface** command is used to display the 802.1p priority to 802.1p priority mappings.

Syntax

show qos dot1p-remap interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port —— The port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IEEE 802.1P remap configuration of all the ports:

```
Device# show qos dot1p-remap interface
```

37.10 show qos dot1p-remap

Note: This command is only available on certain devices.

Description

The **show qos dot1p-remap interface** command is used to display the 802.1p priority to 802.1p priority mappings.

Syntax

show qos dot1p-remap

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IEEE 802.1P remap configuration:

```
Device# show qos dot1p-remap
```

37.11 show qos dscp-map interface

Note: This command is only available on certain devices.

Description

The **show qos dscp-map interface** command is used to display the DSCP priority configuration of the ports.

Syntax

show qos dscp-map interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port —— The port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display theDSCP priority configuration of all the ports:

```
Device# show qos dscp-map interface
```

37.12 show qos dscp-map

Note: This command is only available on certain devices.

Description

The **show qos dscp-map** command is used to display the DSCP priority configuration.

Syntax

show qos dscp-map

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP priority configuration:

```
Device# show qos dscp-map
```

37.13 show qos dscp-remap interface

Note: This command is only available on certain devices.

Description

The **show qos dscp-remap interface** command is used to display the DSCP priority to DSCP priority mappings of the ports.

Syntax

show qos dscp-remap interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port —— The port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP to DSCP mappings for all the ports:

Device# show qos dscp-remap interface

37.14 show qos dscp-remap

Note: This command is only available on certain devices.

Description

The **show qos dscp-remap** command is used to display the DSCP priority to DSCP priority mappings.

Syntax

show qos dscp-remap

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP to DSCP mappings:

Device# show qos dscp-remap

37.15 show qos port-priority interface

Description

The **show qos port-priority interface** command is used to display the port to 802.1p priority mappings for the ports.

Syntax

show qos port-priority interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port to 802.1p priority mappings for all the ports:

```
Device# show qos port-priority interface
```

37.16 show qos trust interface

Description

The **show qos trust interface** command is used to display the trust mode of the ports.

Syntax

show qos trust interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port —— The port number.
port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the trust mode of all the ports:

```
Device# show qos trust interface
```

37.17 show qos queue interface

Description

The **show qos queue interface** command is used to display the scheduler settings of the ports.

Syntax

show qos queue interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port —— The port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the scheduler settings of all the ports:

```
Device# show qos queue interface
```

Chapter 38 Bandwidth Control Commands

Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Rate limit functions to limit the ingress/egress traffic rate on each port. Storm Control function allows the device to monitor broadcast packets, multicast packets and Unknown unicast frames in the network.

38.1 storm-control rate-mode

Description

The **storm-control rate-mode** command is used to configure the storm control mode of the interface. To return to the default configuration, please use **no storm-control rate-mode** command.

Syntax

storm-control rate-mode { kbps | ratio | pps }

no storm-control rate-mode

Parameter

kbps —— Select the storm control mode of the interface as kbps. The device will limit the maximum speed of the specific kinds of traffic in kilo-bits per second.

ratio ——Select the storm control mode of the interface as ratio. The device will limit the percentage of bandwidth utilization for specific kinds of traffic.

pps —— The device will limit the maximum number of packets per second for specific kinds of traffic.

Note: pps is only available on certain devices.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

This command should be used along with the storm-control command to enable the storm control function and specify the detailed parameters.

Example

Set the storm control mode as kbps on port 1/0/5:

```
Device(config)# interface gigabitEthernet 1/0/5
Device(config-if)# storm-control rate-mode kbps
```

38.2 storm-control

Description

The **storm-control** command is used to enable the broadcast, multicast, or unknown unicast strom control function and to set threshold levels on an interface. To return to the default configuration, please use **no storm-control** command.

Syntax

storm-control { broadcast | multicast | unicast } { *rate* }

no storm-control { broadcast | multicast | unicast }

Parameter

broadcast | multicast | unicast —— Select the mode of the storm control on the interface.

rate —— Specify the bandwidth for receiving packets on the port. The specified type of packet traffic exceeding the bandwidth will be processed according to the configuration of **storm-control exceed** command. For kbps, the rate ranges from 1 to 1000000 kbps, and is rounded off to the nearest multiple of 64. For ratio, the rate ranges from 1 to 100 percent. For pps, the rate ranges from 1 to 1488000 packets per second.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Before you configure the storm-control type as kbps or ratio, pelease ensure that the port is not in pps mode.

Example

Configure the broadcast storm control rate as 1024 kbps on port 1/0/5:

```
Device(config)# interface gigabitEthernet 1/0/5
Device(config-if)# storm-control rate-mode kbps
Device(config-if)# storm-control broadcast 1024
```

38.3 storm-control exceed

Description

The **storm-control exceed** command is used to configure the action that the device will perform when the storm exceeds the defined limit on an interface.

Syntax

storm-control exceed { drop | shutdown } [recover-time *time*]

Parameter

drop —— Set the Action as Drop. The port will drop the subsequent packets when the traffic exceeds the limit.

shutdown —— Set the Action as Shutdown. The port will be shutdown when the traffic exceeds the limit.

time ——Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 and the default value is 0. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, which means the port will not recover to its normal state automatically and you can recover the port manually using **storm-control recover** command.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the action as drop on port 1/0/5:

```
Device(config)# interface gigabitEthernet 1/0/5
Device(config-if)# storm-control exceed drop
```

38.4 storm-control recover

Description

The **storm-control recover** command is used to recover the port manually after the port is shutdown because of the storm. When the recover time is specified as 0, the port will not recover to its normal state automatically. In this condition, you need to use this command to recover the port manually.

Syntax

storm-control recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Recover port 1/0/5 manually:

```
Device(config)# interface gigabitEthernet 1/0/5
Device(config-if)# storm-control recover
```

38.5 bandwidth

Description

The **bandwidth** command is used to configure the bandwidth limit for an Ethernet port. To disable the bandwidth limit, please use **no bandwidth** command.

Syntax

bandwidth {[ingress *ingress-rate*] [egress *egress-rate*]}

no bandwidth { all | ingress | egress }

Parameter

ingress-rate —— Specify the upper rate limit for receiving packets. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64.

egress-rate —— Specify the upper rate limit for sending packets. The rate ranges from 1 to 1000000 kbps for the gigaport and 1 to 100000 kbps for the fast port, and is rounded off to the nearest multiple of 64.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ingress-rate as 5120Kbps and egress-rate as 1024Kbps for port 1/0/5:

Device(config)# interface gigabitEthernet 1/0/5

Device(config-if)# bandwidth ingress 5120 **egress** 1024

38.6 show storm-control

Description

The **show storm-control** command is used to display the storm-control information of Ethernet ports.

Syntax

show storm-control interface [fastEthernet *port* | gigabitEthernet *port-list* *ten-gigabitEthernet port* | port-channel *port-channel-id-list*]

Parameter

port-list ——The list of Ethernet ports.

port-channel-id-list —— The list of port channels.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the storm-control information of port 4, 5, 6, and 7:

Device(config)# show storm-control interface gigabitEthernet 1/0/4-7

38.7 show bandwidth

Description

The **show bandwidth** command is used to display the bandwidth-limit information of Ethernet ports.

Syntax

show bandwidth interface [fastEthernet *port* | gigabitEthernet *port-list* ten-gigabitEthernet *port* | port-channel *port-channel-id-list*]

Parameter

port-list ——The list of Ethernet ports.

port-channel-id-list —— The list of port channels.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bandwidth-limit information of port 1/0/4:

```
Device(config)# show bandwidth interface gigabitEthernet 1/0/4
```

Chapter 39 Voice VLAN Commands

Voice VLANs are configured specially for voice data stream. By configuring Voice VLANs and adding the ports with voice devices attached to voice VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

39.1 voice vlan

Description

The **voice vlan** command is used to enable Voice VLAN function. To disable Voice VLAN function, please use **no voice vlan** command.

Syntax

voice vlan *vlan-id*

no voice vlan

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 2 to 4093.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Voice VLAN function for VLAN 10:

```
Device(config)# voice vlan 10
```

39.2 voice vlan (interface)

Description

The **voice vlan** command is used to enable Voice VLAN function on the desired ports. To disable Voice VLAN function on ports, please use **no voice vlan** command.

Syntax

voice vlan

no voice vlan

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Voice VLAN function for port 1/0/1:

```
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)#voice vlan
```

39.3 voice vlan priority

Description

The **voice vlan priority** command is used to configure the priority for the Voice VLAN. To restore to the default priority, please use **no voice vlan priority** command.

Syntax

voice vlan priority *pri*

no voice vlan priority

Parameter

pri—— Priority, ranging from 0 to 7, and the default value is 7.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the priority of the Voice VLAN as 5:

Device(config)# voice vlan priority 5

39.4 voice vlan oui

Description

The **voice vlan oui** command is used to create Voice VLAN OUI. To delete the specified Voice VLAN OUI, please use **no voice vlan oui** command.

Syntax

voice vlan oui *oui-prefix* **oui-desc** *string*

no voice vlan mac-address *oui-prefix*

Parameter

oui-prefix—— The OUI address of the voice device, in the format of XX:XX:XX.

string—— Give a description to the OUI for identification which contains 16 characters at most.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create a Voice VLAN OUI described as TP-Phone with the OUI address 00:11:11:11:11:11 and the mask address FF:FF:FF:00:00:00:

Device(config)#voice vlan oui 00:11:11 **oui-desc** TP-Phone

39.5 show voice vlan

Description

The **show voice vlan** command is used to display the global configuration information of Voice VLAN.

Syntax

show voice vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the configuration information of Voice VLAN globally:

```
Device(config)# show voice vlan
```

39.6 show voice vlan oui-table

Description

The **show voice vlan oui** command is used to display the configuration information of Voice VLAN OUI.

Syntax

show voice vlan oui-table

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the configuration information of Voice VLAN OUI:

```
Device(config)# show voice vlan oui-table
```

39.7 show voice vlan interface

Description

The **show voice vlan interface** command is used to display the Voice VLAN configuration information of all ports.

Syntax

show voice vlan interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the Voice VLAN configuration information of all ports and port channels:

```
Device(config)# show voice vlan interface
```

Chapter 40 Auto VoIP Commands

The Auto VoIP feature is used to prioritize the transmission of voice traffic. Voice over Internet Protocol (VoIP) enables telephone calls over a data network, and the Auto VoIP feature helps provide a classification mechanism for voice packets. When Auto VoIP is configured on a port that receives both voice and data traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is heavy.

40.1 auto-voip

Description

The **auto-voip** command is used to enable the Auto VoIP function globally.

To disable the Auto VoIP function, use **no auto-voip** command.

Syntax

auto-voip

no auto-voip

Command Mode

Global Configuration Mode

Example

Enable the Auto VoIP function globally:

```
Device(config)# auto-voip
```

40.2 auto-voip (interface)

Description

The **auto-voip** command is used to specify the interface mode as VLAN ID for the ports. In this mode, the voice devices will send voice packets with desired VLAN tag.

Syntax

auto-voip *vlan-id*

Parameter

vlan-id——Specify the Auto VoIP VLAN ID. The valid values are from 1 to 4093.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set Auto VoIP VLAN 3 for port 3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# auto-voip 3
```

40.3 auto-voip dot1p

Description

The **auto-voip dot1p** command is used to specify the interface mode as dat1p for the ports. In this mode, the voice devices will send voice packets with desired 802.1p priority.

Syntax

auto-voip dot1p *dot1p*

Parameter

dot1p——Set the 802.1p priority of Auto VoIP on specified ports. It ranges from 0 to 7.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set the 802.1p priority as 5 for the port:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# auto-voip dot1p 5
```

40.4 auto-voip untagged

Description

The **auto-voip untagged** command is used to specify the interface mode as untagged for the ports. In this mode, the voice devices will send untagged voice packets.

Syntax

auto-voip untagged

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set the interface mode as untagged for port 1/0/3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# auto-voip untagged
```

40.5 auto-voip none

Description

The **auto-voip none** command is used to specify the interface mode as none for the ports. In this mode, the device allows the voice devices to use its own configuration to send voice traffic.

Syntax

auto-voip none

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Instruct voice devices that are connected to port 3 to send the packets according to its own configuration:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# auto-voip none
```

40.6 no auto-voip (interface)

Description

The **no auto-voip** command is used to specify the interface mode as disabled for the ports, which means the Auto VoIP function is disabled on the corresponding port.

Syntax

no auto-voip

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Disable the Auto VoIP function on port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# no auto-voip

40.7 auto-voip dscp

Description

The **auto-voip dscp** command is used to set the DSCP value of Auto VoIP on specified ports.

Syntax

auto-voip dscp *value*

Parameter

value——Set the DSCP value of Auto VoIP on specified ports. It ranges from 0 to 63. By default, it is 0.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set DSCP value of Auto VoIP on port 3 as 33:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# auto-voip dscp 33
```

40.8 auto-voip data priority

Description

The **auto-voip data priority** command is used to enable or disable the CoS Override Mode on specified ports.

Syntax

auto-voip data priority { trust | untrust }

Parameter

trust——In this mode, the device will then put the voice packets in the corresponding TC queue according to the 802.1p priority of the packets.

untrust——In this mode, the device will ignore the 802.1p priority in the voice packets and put the packets in TC-5 directly.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Example

Set the CoS Override Mode as trust for port 1/0/3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# auto-voip data priority trust
```

40.9 show auto-voip

Description

The **show auto-voip** command is used to display the Auto VoIP configuration information.

Syntax

show auto-voip [interface]

Parameter

interface —— Displays the Auto VoIP configuration information of ports. When no parameter is entered, displays the global Auto VoIP configuration information.

Command Mode

Privileged EXEC Mode and any Configuration Mode

Example

Displays the global Auto VoIP configuration information:

```
Device (config)# show auto-voip
```

Chapter 41 Access Control Commands

41.1 user access-control ip-based enable

Description

The **user access-control ip-based enable** command is used to configure the access control mode IP-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control ip-based enable

no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the access control mode as IP-based:

```
Device(config)# user access-control ip-based enable
```

41.2 user access-control ip-based

Description

The **user access-control ip-based** command is used to limit the IP-range of the users for login. Only the users within the IP-range you set here are allowed to login. You can add up to 30 IP-based entries. To cancel the user access limit, please use **no user access-control ip-based** command.

Syntax

user access-control ip-based { *ip-addr ip-mask* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control ip-based index *id*

Parameter

ip-addr —— The source IP address. Only the users within the IP-range you set here are allowed for login. 5 IP-based entries can be configured at most.

ip-mask —— The subnet mask of the IP address.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] —— Specify the access interface. These interfaces are enabled by default.

id —— Delete the specified IP-based entry.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the access-control of the user whose IP address is 192.168.0.148:

Device(config)# user access-control ip-based 192.168.0.148

255.255.255.255

41.3 user access-control mac-based enable

Description

The **user access-control mac-based enable** command is used to configure the access control mode MAC-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control mac-based enable

no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the access control mode as MAC-based:

Device(config)# user access-control mac-based enable

41.4 user access-control mac-based

Description

The **user access-control mac-based** command is used to limit the MAC address of the users for login. Only the user with this MAC address you set here is allowed to login. You can add up to 30 mac-based control entries. To delete the mac-based access control entry, please use **no user access-control mac-based** command.

Syntax

user access-control mac-based { *mac-addr* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control mac-based index *id*

Parameter

mac-addr —— The source MAC address. Only the user with this MAC address is allowed to login.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] —— Specify the access interface. These interfaces are enabled by default.

id—— Specify the ID of the mac-based entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure that only the user whose MAC address is 00:00:13:0A:00:01 is allowed to login:

Device(config)# user access-control mac-based 00:00:13:0A:00:01

41.5 user access-control port-based enable

Description

The **user access-control port-based enable** command is used to configure the access control mode Port-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control port-based enable

no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the access control mode as Port-based:

```
Device(config)# user access-control port-based enable
```

41.6 user access-control port-based

Description

The **user access-control port-based** command is used to limit the ports for login. Only the users connected to these ports you set here are allowed to login. You can add up to 30 port-based control entries. To delete the port-based access control entry, please use **no user access-control port-based** command.

Syntax

user access-control port-based interface { gigabitEthernet *port-list*} [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control port-based index *id*

Parameter

port-list——The list group of Ethernet ports, in the format of 1/0/1-4. You can appoint 5 ports at most.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] —— Specify the access interface. These interfaces are enabled by default.

id—— Specify the ID of the port-based entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure that only the users connected to ports 2-6 are allowed to login:

Device(config)# user access-control port-based interface gigabitEthernet 1/0/2-6

Chapter 42 HTTP and HTTPS Commands

With the help of HTTP (HyperText Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer), you can manage the device through a standard browser.
HTTP is the protocol to exchange or transfer hypertext.
SSL (Secure Sockets Layer), a security protocol, is to provide a secure connection for the application layer protocol (e.g. HTTP) based on TCP. Adopting asymmetrical encryption technology, SSL uses key pair to encrypt/decrypt information. A key pair refers to a public key (contained in the certificate) and its corresponding private key. By default the device has a certificate (self-signed certificate) and a corresponding private key. The Certificate/Key Download function enables the user to replace the default key pair.

42.1 ip http server

Description

The **ip http server** command is used to enable the HTTP server within the device. To disable the HTTP function, please use **no ip http server** command. This function is enabled by default. The HTTP and HTTPS server function can be disabled at the same time.

Syntax

ip http server

no ip http server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Disable the HTTP function:

```
Device(config)# no ip http server
```

42.2 ip http port

Description

The **ip http port** command is used to configure the port number of the HTTP server within the device. To set the number to the default value, please use **no ip http port** command.

Syntax

ip http port *port-num*

no ip http port

Parameter

port-num —— Enter the port number. This value ranges from 1 to 65535.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the port number of HTTP server as 1800:

```
Device(config)# ip http port 1800
```

42.3 ip http max-users

Description

The **ip http max-users** command is used to configure the maximum number of users that are allowed to connect to the HTTP server. To cancel this limitation, please use **no ip http max-users** command.

Syntax

ip http max-users *admin-num operator-num poweruser-num user-num*

no ip http max-users

Parameter

admin-num —— The maximum number of the users logging on to the HTTP server as Admin, ranging from 1 to 16. The total number of users should be no more than 16.

operator-num —— The maximum number of the users logging on to the HTTP server as operator, ranging from 0 to 15. The total number of users should be no more than 16.

poweruser-num —— The maximum number of the users logging on to the HTTP server as Power User, ranging from 0 to 15. The total number of users should be no more than 16.

user-num —— The maximum number of the users logging on to the HTTP server as User, ranging from 0 to 15. The total number of users should be no more than 16.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the maximum number of the Admin, Operator, Power User and User as 5, 1, 1, 1 for HTTP:

```
Device(config)# ip http max-users 5 1 1 1
```

42.4 ip http session timeout

Description

The **ip http session timeout** command is used to configure the connection timeout of the HTTP server. To restore to the default timeout time, please use **no ip http session timeout** command.

Syntax

ip http session timeout *time*

no ip http session timeout

Parameter

time ——The timeout time, ranging from 5 to 30 in minutes. By default, the value is 10.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the timeout time of the HTTP connection as 15 minutes:

```
Device(config)# ip http session timeout 15
```

42.5 ip http secure-server

Description

The **ip http secure-server** command is used to enable the HTTPS server within the device. To disable the HTTPS function, please use **no ip http secure-server** command. This function is enabled by default. The HTTP and HTTPS server function can be disabled at the same time.

Syntax

ip http secure-server

no ip http secure-server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the HTTP function:

```
Device(config)# no ip http secure-server
```

42.6 ip http secure-port

Description

The **ip http secure-port** command is used to configure the port number of the HTTPS server within the device. To set the number to the default value, please use **no ip http secure-port** command.

Syntax

ip http secure-port *port-num*

no ip http secure-port

Parameter

port-num —— Enter the port number. This value ranges from 1 to 65535.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the port number of HTTPS server as 2800:

Device(config)# ip http secure-port 2800

42.7 ip http secure-protocol

Description

The **ip http secure-protocol** command is used to configure the SSL protocol version. To restore to the default SSL version, please use **no ip http secure-protocol** command. By default, the device supports all the protocol versions, including SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2.

Syntax

ip http secure-protocol { ssl3 | tls1 | tls11 | tls12 | all }

no ip http secure-protocol

Parameter

ssl3 —— Select SSL Version 3.0 as the protocol for HTTPS.

tls1 —— Select TLS Version 1.0 as the protocol for HTTPS.

tls11 —— Select TLS Version 1.1 as the protocol for HTTPS.

tls12 —— Select TLS Version 1.2 as the protocol for HTTPS.

all —— Enable all the above protocols for HTTPS. The HTTPS server and client will negotiate the protocol each time.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the protocol of SSL connection as SSL 3.0:

Device(config)# ip http secure-protocol ssl3

42.8 ip http secure-ciphersuite

Description

The **ip http secure-ciphersuite** command is used to configure the cipherSuites over the SSL connection supported by the device. To restore to the default ciphersuite types, please use **no ip http secure-ciphersuite** command.

Syntax

ip http secure-ciphersuite { [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] [3des-ede-cbc-sha] [ecdhe-a128-g-s256] [ecdhe-a256-g-s384] }

no ip http secure-ciphersuite

Parameter

[rc4-128-md5] [rc4-128-sha] [des-cbc-sha] [3des-ede-cbc-sha] [ecdhe-a128-g-s256] [ecdhe-a256-g-s384] —— Specify the encryption algorithm and the digest algorithm to use on an SSL connection. By default, the device supports all these ciphersuites.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ciphersuite to be used for encryption over the SSL connection as 3des-ede-cbc-sha:

Device(config)# ip http secure-ciphersuite 3des-ede-cbc-sha

42.9 ip http secure-max-users

Description

The **ip http secure-max-users** command is used to configure the maximum number of users that are allowed to connect to the HTTPs server. To cancel this limitation, please use **no ip http secure-max-users** command.

Syntax

ip http secure-max-users *admin-num operator-num poweruser-num user-num*

no ip secure-max-users

Parameter

admin-num —— The maximum number of the users logging on to the HTTPs server as Admin, ranging from 1 to 16. The total number of users should be less than 16.

Operator-num —— The maximum number of the users logging on to the HTTPs server as operator, ranging from 0 to 15. The total number of users should be less than 16.

poweruser-num —— The maximum number of the users logging on to the HTTP server as Power User, ranging from 0 to 15. The total number of users should be less than 16.

user-num —— The maximum number of the users logging on to the HTTP server as User, ranging from 0 to 15. The total number of users should be less than 16.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of the Admin, Operator, Power User and User as 5, 1, 1, 1 for HTTPs:

```
Device(config)# ip http secure-max-users 5 1 1 1
```

42.10 ip http secure-session timeout

Description

The **ip http secure-session timeout** command is used to configure the connection timeout of the HTTPS server. To restore to the default timeout time, please use **no ip http secure-session timeout** command.

Syntax

ip http secure-session timeout *time*

no ip http secure-session timeout

Parameter

time —— The timeout time, ranging from 5 to 30 in minutes. By default, the value is 10.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the timeout time of the HTTPs connection as 15 minutes:

```
Device(config)# ip http secure-session timeout 15
```

42.11 ip http secure-server download certificate

Description

The **ip http secure-server download certificate** command is used to download a certificate to the device from TFTP server.

Syntax

ip http secure-server download certificate *ssl-cert* **ip-address** *ip-addr*

Parameter

ssl-cert —— The name of the SSL certificate which is selected to download to the device. The length of the name ranges from 1 to 25 characters. The Certificate must be BASE64 encoded.

ip-addr —— The IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download an SSL Certificate named ssl-cert from TFTP server with the IP address of 192.168.0.146:

Device(config)# ip http secure-server download certificate ssl-cert **ip-address** 192.168.0.146

Download an SSL Certificate named ssl-cert from TFTP server with the IP address of fe80::1234

Device(config)# ip http secure-server download certificate ssl-cert **ip-address** fe80::1234

42.12 ip http secure-server download key

Description

The **ip http secure-server download key** command is used to download an SSL key to the device from TFTP server.

Syntax

ip http secure-server download key *ssl-key* **ip-address** *ip-addr*

Parameter

ssl-key —— The name of the SSL key which is selected to download to the device. The length of the name ranges from 1 to 25 characters. The Key must be BASE64 encoded.

ip-addr —— The IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download an SSL key named ssl-key from TFTP server with the IP address of 192.168.0.146:

```
Device(config)# ip http secure-server download key ssl-key ip-address
192.168.0.146
```

Download an SSL key named ssl-key from TFTP server with the IP address of fe80::1234

```
Device(config)# ip http secure-server download key ssl-key ip-address
fe80::1234
```

42.13 show ip http configuration

Description

The **show ip http configuration** command is used to display the configuration information of the HTTP server, including status, session timeout, access-control, max-user number and the idle-timeout, etc.

Syntax

show ip http configuration

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of the HTTP server:

```
Device(config)# show ip http configuration
```

42.14 show ip http secure-server

Description

The **show ip http secure-server** command is used to display the global configuration of SSL.

Syntax

show ip http secure-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSL:

```
Device(config)# show ip http secure-server
```

Chapter 43 SSH Commands

SSH (Security Shell) can provide the unsecured remote management with security and powerful authentication to ensure the security of the management information.

43.1 ip ssh server

Description

The **ip ssh server** command is used to enable SSH function. To disable the SSH function, please use **no ip ssh server** command.

Syntax

ip ssh server

no ip ssh server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the SSH function:

```
Device(config)# ip ssh server
```

43.2 ip ssh port

Description

The **ip ssh port** command is used to configure the port for SSH service. To set the value to the default, please use **no ip ssh port** command.

Syntax

ip ssh port *port*

no ip ssh port

Parameter

port —— Set the port number. It ranges from 1 to 65535. The default value is 22.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the SSH port number as 22:

```
Device(config)# ip ssh port 22
```

43.3 ip ssh version

Description

The **ip ssh version** command is used to enable the SSH protocol version. To disable the protocol version, please use **no ip ssh version** command.

Syntax

ip ssh version { v2 }

no ip ssh version { v2 }

Parameter

v2 —— The SSH protocol version to be enabled. It represents SSH v2.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable SSH v2:

```
Device(config)# ip ssh version v2
```

43.4 ip ssh algorithm

Description

The **ip ssh algorithm** command is used to configure the algorithm in SSH function. To disable the specified algorithm, please use **no ip ssh algorithm** command.

Syntax

ip ssh algorithm { AES-CBC | 3DES-CBC | AES-GCM | AES-CTR | HMAC-SHA1 | HMAC-SHA2 |HMAC-MD5 | UMAC }

no ip ssh algorithm

Parameter

AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 —— Specify the SSH algorithm.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the SSH algorithm as AES128-CBC:

```
Device(config)# ip ssh algorithm AES128-CBC
```

43.5 ip ssh algorithm compatibility

Description

The **ip ssh algorithm compatibility** command is used to configure enable compatibility configuration to allow SSH to use unsafe encryption algorithms.

Syntax

ip ssh algorithm compatibility

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable compatibility configuration to allow SSH to use unsafe encryption algorithms:

Device#ip ssh algorithm compatibility

This command will synchronously enable unsafe algorithms such as

AES-CBC, 3DES-CBC, HMAC-SHA1, HMAC-MD5, etc. (yes/no)

43.6 ip ssh session-timeout

Description

The **ip ssh session-timeout** command is used to specify the idle-timeout time of SSH. To restore to the factory defaults, please use **ip ssh session-timeout** command.

Syntax

ip ssh session-timeout *value*

no ip ssh session-timeout

Parameter

value —— The Idle-timeout time. During this period, the system will automatically release the connection if there is no operation from the client. It ranges from 1 to 120 in seconds. By default, this value is 120 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the idle-timeout time of SSH as 30 seconds:

Device(config)# ip ssh session-timeout 30

43.7 ip ssh max-client

Description

The **ip ssh max-client** command is used to specify the maximum number of the connections to the SSH server. To return to the default configuration, please use **no ip ssh max-client** command.

Syntax

ip ssh max-client *num*

no ip ssh max-client

Parameter

num —— The maximum number of the connections to the SSH server. It ranges from 1 to 5. By default, this value is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the maximum number of the connections to the SSH server as 3:

```
Device(config)# ip ssh max-client 3
```

43.8 ip ssh download

Description

The **ip ssh download** command is used to download the SSH key file from TFTP server.

Syntax

ip ssh download { v1 | v2 } *key-file* **ip-address** *ip-addr*

Parameter

v1 | v2 —— Select the type of SSH key to download, v1 represents SSH-1, v2 represents SSH-2.

key-file —— The name of the key-file which is selected to download. The length of the name ranges from 1 to 25 characters. The key length of the downloaded file must be in the range of 512 to 3072 bits.

ip-addr —— The IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.1 or fe80::1234.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download an SSH-1 type key file named ssh-key from TFTP server with the IP address 192.168.0.148:

Device(config)# ip ssh download v1 ssh-key **ip-address** 192.168.0.148

Download an SSH-1 type key file named ssh-key from TFTP server with the IP address fe80::1234:

Device(config)# ip ssh download v1 ssh-key **ip-address** fe80::1234

43.9 remove public-key

Description

The **remove public-key** command is used to remove the SSH public key from the device.

Syntax

remove public-key { v1 | v2 }

Parameter

v1 | v2 —— Select the type of SSH public key, v1 represents SSH-1, v2 represents SSH-2.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Remove the SSH-1 type public key from the device:

Device# remove public-key v1

43.10 show ip ssh

Description

The **show ip ssh** command is used to display the global configuration of SSH.

Syntax

show ip ssh

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSH:

```
Device(config)# show ip ssh
```

Chapter 44 Telnet Commands

44.1 telnet

Description

The **telnet** command is used to log in and manage other devices via telnet.

Syntax

telnet *ip-addr*

Parameter

ip-addr——The IP address of the device you want to log in.

Command Mode

Privileged EXEC Mode

Privilege Requirement

None.

User Guidelines

Make sure the device can access the device, and the device can be logged in via telnet.

Example

Log in to a device with the IP address of 192.168.0.10:

```
Device# telnet 192.168.0.10
```

44.2 telnet enable

Description

The **telnet enable** command is used to enable the Telnet function. To disable the Telnet function, please use the **telnet disable** command. This function is enabled by default.

Syntax

telnet enable

telnet disable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Disable the Telnet function:

```
Device(config)# telnet disable
```

44.3 telnet port

Description

The **telnet port** command is used to configure the telent port number. To restore the setting, please use the **no telnet port** command.

Syntax

telnet port *port*

no telnet port

Parameter

port——The number of telnet port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the telnet port number as 566:

```
Device(config)# telnet port 566
```

44.4 show telnet-status

Description

The **show telnet-status** command is used to display the configuration information of the Telnet function.

Syntax

show telnet-status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display whether the Telnet function is enabled:

```
Device(config)# show telnet-status
```

Chapter 45 Serial Port Commands

Note: Serial Port commands are only available on certain devices.

45.1 serial_port baud-rate

Description

The **serial_port baud-rate** command is used to configure the communication baud rate on the console port. To return to the default baud rate, please use **no serial_port** command.

Syntax

serial_port baud-rate { 9600 | 19200 | 38400 | 57600 | 115200 }

no serial_port

Parameter

9600 | 19200 | 38400 | 57600 | 115200 ——Specify the communication baud rate on the console port. The default baul rate is 38400 bps.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the communication baud rate on the console port to the default value:

```
Device(config)# no serial_port
```

Chapter 46 Port Security Commands

You can limit the number of MAC addresses that can be learned on each port on this page, thus preventing the MAC address table from being exhausted by the attack packets.

46.1 mac address-table max-mac-count

Description

The **mac address-table max-mac-count** command is used to enable the port security feature of the port and configure the related parameters. To disable the feature and restore the parameters to defaults on the port, please use **no mac address-table max-mac-count** command.

Syntax

mac address-table max-mac-count { [max-number *num*] [exceed-max-learned enable | disable] [mode { dynamic | static | permanent }] [status { forward | drop | disable }] }

no mac address-table max-mac-count [max-number | mode | status]

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the maximum number of MAC addresses that can be learned on port 1/0/3 as 30, enable exceed-max-leaned feature and configure the mode as permanent and the status as drop:

Device (config)#interface gigabitEthernet 1/0/3

Device(config-if)#mac address-table max-mac-count max-number 30 **exceed-maxlearned** enable **mode** permanent **status** drop

46.2 show mac address-table max-mac-count

Description

The **show mac address-table max-mac-count** command is used to display the port security configuration on each port.

Syntax

show mac address-table max-mac-count interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port security configuration on port 1/0/1

Device# show mac address-table max-mac-count interface gigabitEthernet 1/0/1

Chapter 47 Port Mirroring Commands

Port Mirroring allows the device to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic on source ports, LAGs or the CPU. Usually, the monitoring port is connected to data diagnose device, which is used to analyze the monitored packets for monitoring and troubleshooting the network.

47.1 monitor session destination interface

Description

The **monitor session destination interface** command is used to configure the monitoring port. Each monitor session has only one monitoring port. To change the monitoring port, please use the **monitor session destination interface** command by changing the port value. The **no monitor session** command is used to delete the corresponding monitoring port or monitor session.

Syntax

monitor session *session_num* **destination interface gigabitEthernet** *port*

no monitor session *session_num* **destination interface gigabitEthernet** *port*

no monitor session *session_num*

Parameter

session_num —— The monitor session number, can only be specified as 1.

port ——The monitoring port number.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Create monitor session 1 and configure port 1/0/1 as the monitoring port:

```
Device(config)# monitor session 1 destination interface gigabitEthernet
1/0/1
```

Delete the monitoring port 1/0/2 from monitor session 1:

Device(config)# no monitor session 1 **destination interface gigabitEthernet** 1/0/2

Delete the monitor session 1:

Device(config)# no monitor session 1

47.2 monitor session source

Description

The **monitor session source** command is used to configure the monitored interface. To delete the corresponding monitored interface, please use **no monitor session source** command.

Syntax

monitor session *session_num* **source** { cpu *cpu_number* | interface gigabitEthernet *port-list* | interface port-channel *port-channel-id*} *mode*

no monitor session *session_num* **source** { cpu *cpu_number* | interface gigabitEthernet *port-list* | interface port-channel *port-channel-id*} *mode*

Parameter

session_num —— The monitor session number. It can only be specified as 1.

cpu_number —— The CPU number. It can only be specified as 1.

port-list —— List of the Ethernet port number. It is multi-optional.

lag-list —— List of LAG interfaces. It is multi-optional.

mode —— The monitor mode. There are three options: rx, tx and both. Rx (ingress monitoring mode), means the incoming packets received by the monitored interface will be copied to the monitoring port. Tx (egress monitoring mode), indicates the outgoing packets sent by the monitored interface will be copied to the monitoring port. Both (ingress and egress monitoring), presents the incoming packets received and the outgoing packets sent by the monitored interface will both be copied to the monitoring port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

User Guidelines

1. The monitoring port is corresponding to current interface configuration mode.
2. Monitored ports number is not limited, but it can't be the monitoring port at the same time.
3. Whether the monitoring port and monitored ports are in the same VLAN or not is not demanded strictly.
4. The monitoring port and monitored ports cannot be link-aggregation member.

Example

Create monitor session 1, then configure port 4, 5, 7 as monitored port and enable ingress monitoring:

```
Device(config)# monitor session 1 source interface gigabitEthernet
1/0/4-5,1/0/7 rx
```

Delete port 4 in monitor session 1 and its configuration:

```
Device(config)# no monitor session 1 source interface gigabitEthernet
1/0/4 rx
```

47.3 show monitor session

Description

The **show monitor session** command is used to display the configuration of port monitoring.

Syntax

show monitor session [*session_num*]

Parameter

session_num —— The monitor session number, can only be specified as 1. It is optional.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the monitoring configuration of monitor session 1:

```
Device(config)# show monitor session 1
```

Chapter 48 ACL Commands

ACL (Access Control List) is used to filter data packets by configuring a series of match conditions, operations and time ranges. It provides a flexible and secured access control policy and facilitates you to control the network security.

48.1 access-list create

Description

The **access-list create** command is used to create an ACL.

Syntax

access-list create *acl-id* [name *acl-name*]

no access-list create {*acl-id*}

Parameter

acl-id ——Enter an ACL ID. The IDs for MAC ACL are from 0 to 499. The IDs for IP ACL are from 500 to 999. The IDs for Combined ACL are from 1000 to 1499. The IDs for IPv6 ACL are from 1500 to 1999.

Note: Packet Content ACL is only available on certain devices.

acl-name —— Enter a name to identify the ACL.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an IP ACL whose ID is 523:

```
Device(config)# access-list create 523
```

48.2 access-list resequence

Description

The **access-list resequence** command is used to resequence the rules by providing a Start Rule ID and Step value.

Syntax

access-list resequence *acl-id-or-name* **start** *start-rule-id* **step** *rule-id-step-value*

Parameter

acl-id-or-name —— The ACL ID or name.

start-rule-id —— The start rule ID.

rule-id-step-value —— The step value.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Resequence the rules of ACL 12 with the start ID as 1 and step value as 5:

```
Device(config)# access-list resequence 12 start 1 step 5
```

48.3 access-list mac

Description

The **access-list mac** command is used to create MAC ACL. To delete the MAC ACL, please use **no access-list mac**.

Syntax

access-list mac *acl-id-or-name* **rule** { auto | *rule-id*} { deny | permit } **logging** {enable | disable} [smac *source-mac* smask *source-mac-mask*] [dmac *destination-mac* dmask *destination-mac-mask*] [type *ether-type*] [pri *dot1p-priority*] [vid *vlan-id*] [tseg *time-range-name*]

no access-list mac *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

enable | disable —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac —— Enter the source MAC address. The format is FF:FF:FF:FF:FF:FF.

source-mac-mask —— Enter the mask of the source MAC address. This is required if a source MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

destination-mac —— Enter the destination MAC address. The format is FF:FF:FF:FF:FF:FF.

destination-mac-mask —— Enter the mask of the destination MAC address. This is required if a destination MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

ether-type —— Specify an Ethernet-type with 4 hexadecimal numbers.

dot1p-priority: The user priority ranges from 0 to 7. The default is No Limit.

vlan-id —— The VLAN ID ranges from 1 to 4094.

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create MAC ACL 50 and configure Rule 5 to permit packets with source MAC address 00:34:a2:d4:34:b5:

Device (config)#access-list create 50

Device (config-mac-acl)#access-list mac 50 **rule** 5 **permit logging disable**

smac 00:34:a2:d4:34:b5 **smask** ff:ff:ff:ff:ff:ff

48.4 access-list ip

Description

The **access-list ip** command is used to add IP ACL rule. To delete the corresponding rule, please use **no access-list ip** command. IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Syntax

access-list ip *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [sip *sip-address* sip-mask *sip-address-mask*] [dip *dip-address* dip-mask *dip-address-mask*] [dscp *dscp-value*] [tos *tos-value*] [pre *pre-value*] [frag enable | disable] [protocol *protocol* [s-port *s-port-number*] [s-port-mask *s-port-mask*] [d-port *d-port-number*] [d-port-mask *d-port-mask*] [tcpflag *tcpflag*]] [tseg *time-range-name*]

no access-list ip *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

sip-address —— Enter the source IP address.

sip-address-mask —— Enter the mask of the source IP address. This is required if a source IP address is entered.

dip-address —— Enter the destination IP address.

dip-address-mask —— Enter the mask of the destination IP address. This is required if a destination IP address is entered.

dscp-value —— Specify the DSCP value between 0 and 63.

tos-value——Specify an IP ToS value to be matched between 0 and 15.

pre-value——Specify an IP Precedence value to be matched between 0 and 7.

frag {enable | disable}—— Enable or disable matching of fragmented packets. The default is disable. When enabled, the rule will apply to all fragmented packets and always permit to forward the last fragment of a packet.

Note: frag {enable | disable} is only available on certain devices.

protocol—— Specify a protocol type.

s-port-number—— Specify the source port number.

s-port-mask—— Specify the source port mask with 4 hexadecimal numbers.

d-port-number—— Specify the destination port number.

d-port-mask—— Specify the destination port mask with 4 hexadacimal numbers.

tcpflag—— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name—— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create IP ACL 600, and configure Rule 1 to permit packets with source IP address 192.168.1.100:

Device (config)#access-list create 600

Device (config)#access-list ip 600 **rule** 1 permit **logging** disable **sip**

192.168.1.100 **sip-mask** 255.255.255.255

48.5 access-list combined

Description

The **access-list combined** command is used to add Combined ACL rule. To delete the corresponding rule, please use **no access-list extended** command.

Syntax

access-list combined *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [smac *source-mac-address* smask *source-mac-mask*] [dmac *dest-mac-address* dmask *dest-mac-mask*] [vid *vlan-id*] [type *ether-type*] [pri *priority*] [sip *source-ip-address* sip-mask *source-ip-mask*]] [dip *destination-ip-address* dip-mask *destination-ip-mask*] [dscp *dscp-value*] [tos *tos-value*] [pre *pre-value*] [protocol *protocol* [s-port *s-port-number* s-port-mask *s-port-mask*] [d-port *d-port-number* d-port-mask *d-port-mask*] [tcpflag *tcpflag*]] [tseg *time-range-name*]

no access-list combined *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac-address —— Enter the source MAC address.

source-mac-mask —— Enter the source MAC address mask.

dest-mac-address —— Enter the destination MAC address.

dest-mac-mask —— Enter the destination MAC address mask. This is required if a destination MAC address is entered.

vlan-id: The VLAN ID ranges from 1 to 4094.

ether-type —— Specify the Ethernet-type with 4 hexadecimal numbers.

priority —— The user priority ranges from 0 to 7. The default is No Limit.

source-ip: Enter the source IP address.

source-ip-mask —— Enter the mask of the source IP address. It is required if source IP address is entered.

destination-ip —— This is required if a source IP address is entered.

destination-ip-mask —— Enter the destination IP address mask. This is required if a destination IP address is entered.

dscp-value —— Specify the DSCP value between 0 and 63.

tos-value ——Specify an IP ToS value to be matched between 0 and 15.

pre-value ——Specify an IP Precedence value to be matched between 0 and 7.

protocol —— Specify a protocol type.

s-port-number —— Specify the source port number.

s-port-mask —— Specify the source port mask with 4 hexadecimal numbers.

d-port-number —— Specify the destination port number.

d-port-mask —— Specify the destination port mask with 4 hexadecimal numbers.

tcpflag —— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create Combined ACL 1100 and configure Rule 1 to deny packets with source IP address 192.168.3.100 in VLAN 2:

Device(config)# access-list create 1100

Device(config)# access-list combined 1100 **logging** disable **rule** 1 permit **vid** 2 **sip** 192.168.3.100 **sip-mask** 255.255.255.255

48.6 access-list ipv6

Description

The **access-list ipv6** command is used to add IPv6 ACL rule. To delete the corresponding rule, please use **no access-list ipv6** command. IPv6 ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets, the DSCP and flow-label value, etc.

Syntax

access-list ipv6 *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [class *class-value*] [flow-label *flow-label-value*] [sip *source-ip-address* sip-mask *source-ip-mask*] [dip *destination-ip-address* dip-mask *destination-ip-mask*] [s-port *source-port-number*] [d-port *destination-port-number*] [tseg *time-range-name*]

no access-list ipv6 *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

class-value —— Specify a class value to be matched. It ranges from 0 to 63.

flow-label-value —— Specify a Flow Label value to be matched.

source-ip-address —— Enter the source IP address. Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.

source-ip-mask —— Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for

example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

destination-ip-address —— Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 addresses but only the first 64 bits will be valid.

destination-ip-mask: Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

source-port-number —— Enter the TCP/UDP source port if TCP/UDP protocol is selected.

destination-port-number —— Enter the TCP/UDP destination port if TCP/UDP protocol is selected.

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

User Guidelines

Before binding an IPv6 ACL to a VLAN or interface, you should configure the SDM template as “enterpriseV6” and save your configurations.

Example

Create IPv6 ACL 1600 and configure Rule 1 to deny packets with source IPv6 address CDCD:910A:2222:5498:8475:1111:3900:2020:

Device(config)# access-list create 1600

Device(config)# access-list ipv6 1600 rule 1 deny **logging** disable **sip**

CDCD:910A:2222:5498:8475:1111:3900:2020 **sip-mask** ffff:ffff:ffff:ffff

48.7 access-list action

Description

The **access-list action** command is used to specify a rule to be configured with policies and enter Action Configuration mode. To delete the corresponding policies, please use **no access-list action** command.

Syntax

access-list action *acl-id-or-name* **rule** *rule-id*

no access-list action *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL.

rule-id —— Enter the ID of the ACL rule.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify the rule 1 of ACL 200 to be configured with policies:

```
Device(config)# access-list action 200 rule 1
```

48.8 redirect

Description

The **redirect interface** command is used to define the policy to redirect the matched packets to the desired port. To disable this policy, please use **no redirect interface** command.

Syntax

redirect interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }

no redirect interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }

Parameter

port —— The destination port to which the packets will be redirected. The default is All.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Define the policy to redirect the matched packets to port 1/0/1 for rule 1 of ACL 6:

```
Device(config)# access-list action 6 rule 1
Device(config-action)# redirect interface gigabitEthernet 1/0/1
```

48.9 traffic

Description

The **traffic** command is used to limit the rate of the matched packets. To restore the settings to the defaults, please use **no traffic**.

Syntax

traffic *traffic-id*

traffic *traffic-name*

Parameter

traffic-id—— The id of the traffic profile.

traffic-name—— The name of the traffic profile.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a policy for rule 1 of ACL 6: limit the transmission rate of the matched packets:

```
Device(config)#access-list action 6 rule 1
Device(config-action)# traffic 1
```

48.10 s-mirror

Description

The **s-mirror** command is used to define the policy to mirror the matched packets to the desired port. To disable this policy, please use **no s-mirror** command.

Syntax

s-mirror interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }

Parameter

port —— The destination port to which the packets will be mirrored.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a policy for rule 1 of ACL 6: specify the mirror port as Gigabit Ethernet port 1/0/2 for the data packets matching this rule:

Device(config)#access-list action 6 **rule** 1

Device(config-action)#s-mirror interface gigabitEthernet 1/0/2

48.11 qos-remark

Description

The **qos-remark** command is used to configure QoS Remark function of policy action. To restore the settings to the default, please use no **qos-remark**.

Syntax

qos-remark [dscp *dscp*] [priority *pri*] [dot1p dot1p-pri]

no qos-remark

Parameter

dscp —— DSCP of QoS Remark. Specify the DSCP region for the data packets matching the corresponding ACL. DSCP ranges from 0 to 63. By default, it is not limited.

pri —— Local Priority of QoS Remark. Specify the local priority for the data packets matching the corresponding ACL. Local Priority ranges from 0 to 7.

dot1p-pri —— 802.1P priority of QoS Remark. This remark configuration will change the data packet's 802.1P priority field to the dot1p-pri you set. 802.1P priority ranges from 0 to 7.

Note: The DSCP and dot1p cannot be configured at the same time.

Command Mode

Action Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure a policy for rule 1 of ACL 6: specify the DSCP region as 30 and local priority 2 for the packets matching this rule:

Device(config)#access-list action 6 **rule** 1

Device(config-action)# qos-remark dscp 30 **priority** 2

48.12 access bind

Description

The **access-list policy name** command is used to add Policy. To delete the corresponding Policy, please use **no access-list policy name** command. A Policy is used to control the data packets those match the corresponding ACL rules.

Syntax

access-list bind *acl-id-or-name* **interface** { [vlan *vlan-list*] | [gpon *port-list*] | [fastEthernet *port-list*] | [gigabitEthernet *port-list*] | [ten-gigabitEthernet *port-list*] }

no access-list bind *acl-id-or-name* **interface** { [vlan *vlan-list*] | [fastEthernet *port-list*] | [gigabitEthernet *port-list*] | [ten-gigabitEthernet *port-list*] }

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

vlan-list —— Specify the ID or the ID list of the VLAN(s) that you want to bind the ACL to. The valid values are from 1 to 4094, for example, 2-3,5.

port-list —— Specify the number or the list of the Ethernet port that you want to bind the ACL to.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind ACL 1 to port 3 and VLAN 4:

```
Device(config)#access-list bind 1 interface vlan 4 gigabitEthernet 1/0/3
```

48.13 show access-list

Description

The **show access-list** command is used to display configuration of ACL.

Syntax

show access-list *acl-id-or-name*

Parameter

acl-id-or-name —— The ID or name of the ACL selected to display the configuration.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the MAC ACL whose ID is 20:

```
Device(config)# show access-list 20
```

48.14 show access-list bind

Description

The **show access-list bind** command is used to display the configuration of ACL binding.

Syntax

show access-list bind

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Policy bind:

```
Device(config)# show access-list bind
```

48.15 show access-list status

Description

The **show access-list status** command is used to display usage status of ACL entry resource.

Syntax

show access-list status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the usage status of ACL entry resource:

```
Device(config)# show access-list status
```

48.16 show access-list counter

Description

The **show access-list counter** command is used to display the packet counter of a specified ACL.

Syntax

show access-list *acl-id-or-name* **counter**

Parameter

acl-id-or-name —— The ID or name of the ACL to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the packet counter of ACL 100:

```
Device(config)# show access-list 100 counter
```

48.17 clear access-list

Description

The **clear access-list** command is used to clear the counter of matched packets of a specified ACL or rule.

Syntax

clear access-list *acl-id-or-name* [rule *rule-id*]

Parameter

acl-id-or-name —— The ID or name of the ACL.

rule-id—— The ID of the rule.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the packet counter of ACL 100:

```
Device(config)# clear access-list 100
```

Chapter 49 DHCPv4 Filter Commands

DHCPv4 Filter function allows the user to not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

49.1 ip dhcp filter

Description

The **ip dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCP Filter function globally, please use **no ip dhcp filter** command.

Syntax

ip dhcp filter

no ip dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Filter function globally:

```
Device(config)#ip dhcp filter
```

49.2 ip dhcp filter (interface)

Description

The **ip dhcp filter (interface)** command is used to enable DHCP Filter function on a specified port. To disable DHCP Filter function on this port, please use **no ip dhcp filter (interface)** command.

Syntax

ip dhcp filter

no ip dhcp filter

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Filter on port 1/0/1

```
Device(config)#interface gigabitEthernet 1/0/1
Device(Config-if)#ip dhcp filter
```

49.3 ip dhcp filter mac-verify

Description

The **ip dhcp filter mac-verify** command is used to enable the MAC Verify feature. To disable the MAC Verify feature, please use **no ip dhcp filter mac-verify** command. There are two fields of the DHCP packet containing the MAC address of the Host. The MAC Verify feature is to compare the two fields and discard the packet if the two fields are different.

Syntax

ip dhcp filter mac-verify

no ip dhcp filter mac-verify

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MAC Verify feature for the Gigabit Ethernet port 10/2:

```
Device(config)#interface gigabitEthernet 1/0/2
Device(config-if)#ip dhcp filter mac-verify
```

49.4 ip dhcp filter limit rate

Description

The **ip dhcp filter limit rate** command is used to enable the Flow Control feature for the DHCP packets. The excessive DHCP packets will be discarded. To restore to the default configuration, please use **no ip dhcp filter limit rate** command.

Syntax

ip dhcp filter limit rate *value*

no ip dhcp filter limit rate

Parameter

value —— The value of Flow Control. The options are 5/10/15/20/25/30 (packet/second). The default value is 0, which stands for "disable".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the Flow Control of GigabitEthernet port 2 as 20 pps:

```
Device(config)#interface gigabitEthernet 1/0/2
Device(config-if)#ip dhcp filter limit rate 20
```

49.5 ip dhcp filter decline rate

Description

The **ip dhcp filter decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decine packets. The excessive DHCP Decline packets will be discarded. To disable the Decline Protect feature, please use **no ip dhcp filter decline rate** command.

Syntax

ip dhcp filter decline rate *value*

no ip dhcp filter decline rate

Parameter

value —— Specify the rate limit of DHCP Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). It default value is 0, which stands for “disable”.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the rate limit of DHCP Decline packets as 20 packets per second on Gigabit Ethernet port 1/0/2:

```
Device(config)#interface gigabitEthernet 1/0/2
Device(config-if)#ip dhcp filter decline 20
```

49.6 ip dhcp filter server permit-entry

Description

The **ip dhcp filter server permit-entry** command is used to add entry for the legal DHCP server. To restore to the default option, please use **no ip dhcp filter server permit-entry** command.

Syntax

ip dhcp filter server permit-entry server-ip *ipAddr* **client-mac** *macAddr* **interface** { fastEthernet *port* | gigabitEthernet port | ten-gigabitEthernet *port* | interface port-channel *port-channel-id*}

no ip dhcp filter server permit-entry server-ip *ipAddr* **client-mac** *macAddr* **interface** { fastEthernet *port* | gigabitEthernet port | ten-gigabitEthernet *port* | interface port-channel *port-channel-id*}

Parameter

ipAddr —— Specify the IP address of the legal DHCPv4 server.

macAddr —— Specify the MAC address of the DHCP Client. The value "all" means all client mac addresses.

port / *port-channel-id* —— Specify the port that the legal DHCPv4 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an entry for the legal DHCPv4 server whose IP address is 192.168.0.100 and connected port number is 1/0/1 without client MAC address restricted:

Device(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100 **client-mac** all **interface gigabitEthernet** 1/0/1

49.7 show ip dhcp filter

Description

The **show ip dhcp filter** command is used to display the configuration of DHCP Filter.

Syntax

show ip dhcp filter

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration:

```
Device#show ip dhcp filter
```

49.8 show ip dhcp filter interface

Description

The **show ip dhcp filter interface** command is used to display the configuration of DHCP Filter on ports.

Syntax

show ip dhcp filter interface [fastEthernet *port*| gigabitEthernet *port*| ten-gigabitEthernet *port*| port-channel *port-channel-id*| gpon port]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration on port 1/0/3:

```
Device#show ip dhcp filter interface gigabitEthernet 1/0/3
```

49.9 show ip dhcp filter server permit-entry

Description

The **show ip dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

show ip dhcp filter server permit-entry

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCP server configuration:

```
Device#show ip dhcp filter server permit-entry
```

Chapter 50 DHCPv6 Filter Commands

DHCPv6 Filter function allows the user to not only to restrict all DHCPv6 Server packets but also to receive any specified DHCPv6 server packet by any specified DHCPv6 client, it is useful when one or more DHCPv6 servers are present on the network and both provide DHCPv6 services to different distinct groups of clients.

50.1 ipv6 dhcp filter

Description

The **ipv6 dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCPv6 Filter function globally, please use **no ipv6 dhcp filter** command.

Syntax

Ipv6 dhcp filter

no ipv6 dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Filter function globally:

```
Device(config)#ipv6 dhcp filter
```

50.2 ipv6 dhcp filter (interface)

Description

The **ipv6 dhcp filter (interface)** command is used to enable DHCPv6 Filter function on a specified port. To disable DHCPv6v Filter function on this port, please use **no ipv6 dhcp filter (interface)** command.

Syntax

ipv6 dhcp filter

no ipv6 dhcp filter

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Filter on port 1/0/1

Device(config)#interface gigabitEthernet 1/0/1

Device(config-if)#ipv6 dhcp filter

50.3 ipv6 dhcp filter limit rate

Description

The **ipv6 dhcp filter limit rate** command is used to enable the Flow Control feature for the DHCPv6 packets. The excessive DHCPv6 packets will be discarded. To restore to the default configuration, please use **no ipv6 dhcp filter limit rate** command.

Syntax

Ipv6 dhcp filter limit rate *value*

no ipv6 dhcp filter limit rate

Parameter

value —— The value of Flow Control. The options are 5/10/15/20/25/30 (packet/second). The default value is 0, which stands for “disable”.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the Flow Control of GigabitEthernet port 2 as 20 pps:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)#ipv6 dhcp filter limit rate 20

50.4 ipv6 dhcp filter decline rate

Description

The **ipv6 dhcp filter decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decine packets. The excessive DHCPv6 Decline packets will be discarded. To disable the Decline Protect feature, please use **no ipv6 dhcp filter decline rate** command.

Syntax

Ipv6 dhcp filter decline rate *value*

no ipv6 dhcp filter decline rate

Parameter

value —— Specify the rate limit of DHCPv6 Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). It default value is 0, which stands for “disable”.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel / interface gpon / interface range gpon)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the rate limit of DHCPv6 Decline packets as 20 packets per second on Gigabit Ethernet port 1/0/2:

Device(config)#interface gigabitEthernet 1/0/2

Device(config-if)#ipv6 dhcp filter decline 20

50.5 ipv6 dhcp filter server permit-entry

Description

The **ipv6 dhcp filter server permit-entry** command is used to add entry for the legal DHCPv6 server. To restore to the default option, please use **no ipv6 dhcp filter server permit-entry** command.

Syntax

Ipv6 dhcp filter server permit-entry server-ip *ipAddr* **interface** { fastEthernet *port* | gigabitEthernet port | ten-gigabitEthernet *port* | interface port-channel *port-channel-id*}

no ipv6 dhcp filter server permit-entry server-ip *ipAddr* **interface** { fastEthernet *port* | gigabitEthernet port | ten-gigabitEthernet *port* | interface port-channel *port-channel-id*}

Parameter

ipAddr —— Specify the IPv6 address of the legal DHCPv6 server.

port-list | *port-channel-id* —— Specify the port that the legal DHCPv6 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an entry for the legal DHCPv6 server whose IP address is 2003::1 and connected port number is 1/0/1:

Device(config)#ipv6 dhcp filter server permit-entry server-ip 2003::1

interface gigabitEthernet 1/0/1

50.6 show ipv6 dhcp filter

Description

The **show ipv6 dhcp filter** command is used to display the configuration of DHCPv6 Filter.

Syntax

show ipv6 dhcp filter

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration:

Device#show ipv6 dhcp filter

50.7 show ipv6 dhcp filter interface

Description

The **show ipv6 dhcp filter interface** command is used to display the configuration of DHCPv6 Filter on ports.

Syntax

show ipv6 dhcp filter interface [[information interface][fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id* | gpon port]]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration on port 1/0/3:

Device#show ipv6 dhcp filter interface gigabitEthernet 1/0/3

50.8 show ip dhcp filter server permit-entry

Description

The **show ipv6 dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

show ipv6 dhcp filter server permit-entry

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCPv6 server configuration:

```
Device#show ipv6 dhcp filter server permit-entry
```

Chapter 51 Ethernet OAM Commands

Ethernet OAM (standing for Operation, Administration, and Maintenance) is Layer 2 protocol that is used for monitoring and troubleshooting Ethernet networks. It can report the network status to network administrators through the OAMPDUs exchanged between two OAM entities. The operation of OAM on an Ethernet interface does not adversely affect data traffic as OAM is a slow protocol with very limited bandwidth potential.

51.1 ethernet-oam

Description

The **ethernet-oam** command is used to enable the Ethernet OAM function for the desired port. To disable the Ethernet OAM function, please use **no ethernet-oam** command.

Syntax

ethernet-oam

no ethernet-oam

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the Ethernet OAM function for Gigabit Ethernet port 1/0/2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)#ethernet-oam

51.2 ethernet-oam mode

Description

The **ethernet-oam mode** command is used to configure the OAM mode for the desired port. To return to the default configurations, please use **no ethernet-oam mode** command. The default mode is active.

Syntax

ethernet-oam mode { passive | active }

no ethernet-oam mode

Parameter

passive —— Specify the OAM mode as passive.

active ——Specify the OAM mode as active.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure Ethernet OAM client to operate in passive mode for Gigabit Ethernet port 2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)#ethernet-oam mode passive

51.3 ethernet-oam link-monitor symbol-period

Description

The **ethernet-oam link-monitor symbol-period** command is used to configure the parameters about one of the link events, error symbol period event. To return to the default configurations, please use **no ethernet-oam link-monitor symbol-period** command.

Syntax

ethernet-oam link-monitor symbol-period { threshold *threshold* | window *window* | notify { disable | enable }}

no ethernet-oam link-monitor symbol-period { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error symbol-period event. The range is from 1 to 4294967295 and the default value is 1.

window —— Configure the error symbol-period event detection interval. The range is from 10 to 600, in terms of 100 ms intervals. The default value is 10.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error symbol-period event, configure the error threshold as 5 and the event detection interval as 3 seconds on Gigabit Ethernet port 1/0/2:

Device(config)# interface gigabitEthernet 1/0/2

Device(config-if)# ethernet-oam link-monitor symbol-period threshold 5

window 30

51.4 ethernet-oam link-monitor frame

Description

The **ethernet-oam link-monitor frame** command is used to configure the parameters about one of the link events, error frame event. To return to the default configurations, please use **no ethernet-oam link-monitor frame** command.

Syntax

ethernet-oam link-monitor frame { [threshold *threshold*] [window *window*] [notify { disable | enable }] }

no ethernet-oam link-monitor frame { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error frame event. The range is from 1 to 4294967295 and the default value is 1.

window —— Configure the error symbol-period event detection interval. The range is from 10 to 600, in terms of 100 ms intervals. The default value is 10.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error frame event, configure the error threshold as 6 and the event detection interval as 9 seconds on Gigabit Ethernet port 1/0/3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# ethernet-oam link-monitor frame threshold 6 window
90
```

51.5 ethernet-oam link-monitor frame-period

Description

The **ethernet-oam link-monitor frame-period** command is used to configure the parameters about one of the link events, error frame period event. To return to the default configurations, please use **no ethernet-oam link-monitor frame-period** command.

Syntax

ethernet-oam link-monitor frame-period { [threshold *threshold*] [window *window*] [notify { disable | enable }] }

no ethernet-oam link-monitor frame-period { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error frame period event. The range is from 1 to 4294967295 and the default value is 1.

window —— Configure the error frame period event detection interval. The range is from 148810 to 89286000. The default value is 148810 for Fast Ethernet port, the default value is 1488100 for Gigabit Ethernet port, and the default value is 14881000 for Ten-Gigabit Ethernet port.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error frame period event, configure the error threshold as 1 and the event detection interval as 148810 frames on Gigabit Ethernet port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# ethernet-oam link-monitor frame-period threshold 1

window 148810

51.6 ethernet-oam link-monitor frame-seconds

Description

The **ethernet-oam link-monitor frame-seconds** command is used to configure the parameters about one of the link events, error frame seconds event. To return to the default configurations, please use **no ethernet-oam link-monitor frame-seconds** command.

Syntax

ethernet-oam link-monitor frame-seconds { [threshold *threshold*] [window *window*] [notify { disable | enable }] }

no ethernet-oam link-monitor frame-seconds { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error frame seconds event. The range is from 1 to 900 and the default value is 1.

window —— Configure the error frame seconds event detection interval. The range is from 100 to 9000, in terms of 100 ms intervals. The default value is 600.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

For error frame seconds event, configure the error threshold as 8 and the event detection interval as 30 seconds on Gigabit Ethernet port 5:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# ethernet-oam link-monitor frame-seconds threshold 8

window 300

51.7 ethernet-oam remote-failure

Description

The ethernet-oam remote-failure command is used to configure whether to notify the link faults or not. The link faults include dying gasp and critical event. To return to the default configurations, please use **no ethernet-oam remote-failure** command.

Syntax

ethernet-oam remote-failure { dying-gasp | critical-event } **notify** { disable | enable }

no ethernet-oam remote-failure { dying-gasp | critical-event } **notify**

Parameter

dying-gasp —— Dying Gasp link event. Dying gasp means an unrecoverable fault, such as power failure, occurs.

critical-event —— Critical Event. Critical-event means unspecified critical event occurs.

notify ——Enable/Disable the event notification. By default, it is enabled.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Disable the Dying Gasp link event notification on Gigabit Ethernet port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# ethernet-oam remote-failure dying-gasp **notify** disable

51.8 ethernet-oam remote-loopback received-remote- loopback

Description

The **ethernet-oam remote-loopback received-remote-loopback** command is used to configure the client to process or to ignore the received remote loopback request. To return to the default configurations, please use **no ethernet-oam remote-loopback received-remote-loopback** command.

Syntax

ethernet-oam remote-loopback received-remote-loopback { process | ignore }

no ethernet-oam remote-loopback received-remote-loopback

Parameter

process —— Process the received remote loopback request.

ignore —— Ignore the received remote loopback request.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the client to process the received remote loopback request on Gigabit Ethernet port 1:

Device(config)# interface gigabitEthernet 1/0/1

Device(config-if)# ethernet-oam remote-loopback received

-remote-loopback process

51.9 ethernet-oam remote-loopback

Description

The **ethernet-oam remote-loopback** command is used to request the remote peer to start or stop the Ethernet OAM remote loopback mode.

Syntax

ethernet-oam remote-loopback { start | stop }

Parameter

start —— Request the remote peer to start the Ethernet OAM remote loopback mode.

stop —— Request the remote peer to stop the Ethernet OAM remote loopback mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Request the remote peer to start the Ethernet OAM remote loopback mode on Gigabit Ethernet port 1/0/3:

Device(config)# interface gigabitEthernet 1/0/3

Device(config-if)# ethernet-oam remote-loopback start

51.10 clear ethernet-oam statistics

Description

The **clear ethernet-oam statistics** command is used to clear Ethernet OAM statistics.

Syntax

clear ethernet-oam statistics [interface gigabitEthernet *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM statistics of all ports are cleared.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Clear Ethernet OAM statistics of Gigabit Ethernet port 1/0/3:

```
Device(config)# clear ethernet-oam statistics interface gigabit Ethernet
1/0/3
```

51.11 clear ethernet-oam event-log

Description

The **clear ethernet-oam event-log** command is used to clear the Ethernet OAM event log.

Syntax

clear ethernet-oam event-log [interface gigabitEthernet *port*]

Parameter

port ——The Gigabit Ethernet port number. By default, the Ethernet OAM event logs of all ports are cleared.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Clear Ethernet OAM event log of Gigabit Ethernet port 1/0/3:

Device(config)# clear ethernet-oam event-log interface gigabitEthernet 1/0/3

51.12 show ethernet-oam configuration

Description

The **show ethernet-oam configuration** command is used to display Ethernet OAM configuration information.

Syntax

show ethernet-oam configuration [interface gigabitEthernet *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM configuration information of all ports is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM configuration information of Gigabit Ethernet port 1/0/2:

Device(config)# show ethernet-oam configuration interface gigabitEthernet 1/0/2

51.13 show ethernet-oam event-log

Description

The **show ethernet-oam event-log** command is used to display the Ethernet OAM event log.

Syntax

show ethernet-oam event-log [interface gigabitEthernet *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM event logs of all ports are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM event log of Gigabit Ethernet port 1/0/2:

```
Device(config)# show ethernet-oam event-log interface gigabitEthernet
1/0/2
```

51.14 show ethernet-oam statistics

Description

The **show ethernet-oam statistics** command is used to display the Ethernet OAM statistics.

Syntax

show ethernet-oam statistics [interface gigabitEthernet *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM statistics of all ports are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM statistics of Gigabit Ethernet port 1/0/2:

```
Device(config)# show ethernet-oam statistics interface gigabitEthernet
1/0/2
```

51.15 show ethernet-oam status

Description

The **show ethernet-oam status** command is used to display the Ethernet OAM status of both the local and the remote client.

Syntax

show ethernet-oam status [interface gigabitEthernet *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM status of all ports is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Display Ethernet OAM status of Gigabit Ethernet port 1/0/2:

```
Device(config)# show ethernet-oam status interface gigabitEthernet
1/0/2
```

Chapter 52 DLDP Commands (Only for Certain Devices)

DLDP (Device Link Detection Protocol) is used to monitor the link state of fiber-optic or twisted-pair Ethernet cables. When a unidirectional link is detected, the corresponding port will be shut down automatically or manually (depending on the shut mode configured).

52.1 dldp (global)

Description

The **dldp** command is used to enable the DLDP function globally. To disable it, please use **no dldp** command.

Syntax

dldp

no dldp

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the DLDP function globally:

```
Device(config)# dldp
```

52.2 dldp interval

Description

The **dldp interval** command is used to define the interval of sending advertisement packets on ports that are in the advertisement state.

Syntax

dldp interval *interval-time*

Parameter

interval-time —— The interval of sending advertisement packets. It ranges from 1 to 30 seconds. By default, it is 5 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the interval of sending advertisement packets as 10 seconds:

```
Device(config)# dldp interval 10
```

52.3 dldp shut-mode

Description

The **dldp shut-mode** command is used to configure the shutdown mode when a unidirectional link is detected.

Syntax

dldp shut-mode { auto | manual }

Parameter

auto —— The device automatically shuts down ports when a unidirectional link is detected. By default, the shut-mode is auto.

manual ——The device displays an alert when a unidirectional link is detected. The operation to shut down the unidirectional link ports is accomplished by the users.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the shut-mode as manual:

```
Device(config)# dldp shut-mode manual
```

52.4 dldp reset (global)

Note: This command is only available on certain devices

Description

The **dldp reset** command is used to reset all the unidirectional links and restart the link detect process.

Syntax

dldp reset

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Reset the DLDP function globally:

```
Device(config)# dldp reset
```

52.5 dldp(interface)

Description

The **dldp** command is used to enable the DLDP function of the specified port. To disable it, please use **no dldp** command.

Syntax

dldp

no dldp

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the DLDP function of ports 1/0/2-4:

```
Device (config)# interface range gigabitEthernet 1/0/2-4
Device (config-if-range)# dldp
```

52.6 show dldp

Description

The **show dldp** command is used to display the global configuration of DLDP function such as DLDP global state, DLDP interval and shut mode.

Syntax

show dldp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of DLDP function:

```
Device# show dldp
```

52.7 show dldp interface

Description

The **show dldp interface** command is used to display the configuration and state of all the Ethernet ports.

Syntax

show dldp interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration and state of all ports:

```
Device# show dldp interface
```

Chapter 53 SNMP Commands

SNMP (Simple Network Management Protocol) functions are used to manage the network devices for a smooth communication, which can facilitate the network administrators to monitor the network nodes and implement the proper operation.

53.1 snmp-server

Description

The **snmp-server** command is used to enable the SNMP function. By default, it is disabled. To return to the default configuration, please use **no snmp-server** command.

Syntax

snmp-server

no snmp-server

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the SNMP function:

```
Device(config)# snmp-server
```

53.2 snmp-server view

Description

The **snmp-server view** command is used to add View. To delete the corresponding View, please use **no snmp-server view** command. The OID (Object Identifier) of the SNMP packets is used to describe the managed objects of the device, and the MIB (Management Information Base) is the set of the OIDs. The SNMP View is created for the SNMP management station to manage MIB objects.

Syntax

snmp-server view *name mib-oid* { include | exclude }

no snmp-server view *name mib-oid*

Parameter

name —— The entry name of View, ranging from 1 to 16 characters. Each View includes several entries with the same name.

mib-oid —— MIB Object ID. It is the Object Identifier (OID) for the entry of View, ranging from 1 to 61 characters.

include | exclude —— View Type, with include and exclude options. They represent the view entry can/cannot be managed by the SNMP management station individually.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a View named view1, configuring the OID as 1.3.6.1.6.3.20, and this OID can be managed by the SNMP management station:

```
Device(config)# snmp-server view view1 1.3.6.1.6.3.20 include
```

53.3 snmp-server group

Description

The **snmp-server group** command is used to manage and configure the SNMP group. To delete the corresponding SNMP group, please use **no snmp-server group** command. SNMP v3 provides the VACM (View-based Access Control Model) and USM (User-Based Security Model) mechanisms for authentication. The users in the SNMP Group can manage the device via the Read View, Write View and Notify View. And the authentication mode and the privacy mode guarantee the high security for the communication between the management station and the managed device.

Syntax

snmp-server group *name* [smode v3] [slev { noAuthNoPriv | authNoPriv | authPriv }] [read *read-view*] [write *write-view*] [notify *notify-view*]

no snmp-server group *name* **smode** v3 **slev** { noAuthNoPriv | authNoPriv | authPriv }

Parameter

name ——The SNMP Group name, ranging from 1 to 16 characters. The Group Name, Security Model and Security Level compose the identifier of the

SNMP Group. These three items of the Users in one group should be the same.

v3 —— The security mode for the group, v3 indicates SNMPv3, the most secure level.

slev —— The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). By default, the Security Level is noAuthNoPriv. There is no need to configure this in SNMP v1 Mode and SNMP v2c Mode.

read-view —— Select the View to be the Read View. The management access is restricted to read-only, and changes cannot be made to the assigned SNMP View.

write-view —— Select the View to be the Write View. The management access is writing only and changes can be made to the assigned SNMP View. The View defined both as the Read View and the Write View can be read and modified.

notify-view —— Select the View to be the Notify View. The management station can receive notification messages of the assigned SNMP view generated by the device's SNMP agent.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a group, and configure the name as group 1, the Security Model as SNMP v3, the security level as authNoPriv, the management access to the assigned View viewDefault as read-write, besides the notification messages sent by View viewDefault can be received by Management station:

Device(config)# snmp-server group group1 **smode** v3 **slev** authNoPriv **read** viewDefault **write** viewDefault **notify** viewDefault

Delete group 1:

Device(config)# no snmp-server group group1 **smode** v3 **slev** authNoPriv

53.4 snmp-server user

Description

The **snmp-server user** command is used to add User. To delete the corresponding User, please use **no snmp-server user** command. The User in an SNMP Group can manage the device via the management station software. The User and its Group have the same security level and access right.

Syntax

snmp-server user *name* { local | remote } *group-name* [smode v3] [slev noAuthNoPriv] [cmode none] [cpwd *confirm-pwd*] [emode none] [epwd *encrypt-pwd*]

snmp-server user *name* { local | remote } *group-name* [smode v3] **slev** authNoPriv **cmode** { MD5 | SHA } **cpwd** *confirm-pwd* [emode none] [epwd *encrypt-pwd*]

snmp-server user *name* { local | remote } *group-name* [smode v3] **slev** authPriv **cmode** { MD5 | SHA } **cpwd** *confirm-pwd* **emode** DES **epwd** *encrypt-pwd*

no snmp-server user *name*

Parameter

name —— User Name, ranging from 1 to 30 characters.

local | remote —— User Type, with local and remote options. Local indicates that the user is connected to a local SNMP engine, while remote means that the user is connected to a remote SNMP engine. As the remote engine ID and user password are used to compute the authentication and privacy digests, before configuring a remote user, you need to set the remote engine ID first.

group-name —— The Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

v3 ——The security mode for the user. v3 indicates SNMPv3, the most secure model.

slev —— The Security Level of SNMP v3 User. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and

encrypt packets). The security level from lowest to highest is: noAuthNoPriv, authNoPriv, authPriv, and the default is noAuthNoPriv. The security level of the user should not be lower than the group it belongs to.

cmode —— The Authentication Mode of the SNMP v3 User, with none, MD5 and SHA options. None indicates no authentication method is used, MD5 indicates the port authentication is performed via HMAC-MD5 algorithm and SHA indicates the port authentication is performed via SHA (Secure Hash Algorithm). SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is "none".

confirm-pwd —— Authentication Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

emode —— The Privacy Mode of the SNMP v3 User, with none and DES options. None indicates no privacy method is used, and DES indicates DES encryption method is used. By default, the Privacy Mode is "none".

encrypt-pwd —— Privacy Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add Local User admin to Group group2, and configure the Security Model of the user as v3, the Security Level of the group as authPriv, the Authentication Mode of the user as MD5, the Authentication Password as 11111, the Privacy Mode as DES, and the Privacy Password as 22222:

Device(config)# snmp-server user admin local group2 **smode** v3 **slev** authPriv **cmode** MD5 **cpwd** 11111 **emode** DES **epwd** 22222

53.5 snmp-server community

Description

The **snmp-server community** command is used to add Community. To delete the corresponding Community, please use **no snmp-server community** command. SNMP v1 and SNMP v2c adopt community name

authentication. The community name can limit access to the SNMP agent from SNMP network management station, functioning as a password.

Syntax

snmp-server community *name* { read-only | read-write } *mib-view*

no snmp-server community *name*

Parameter

name —— Community Name, ranging from 1 to 255 characters.

read-only | read-write —— The access rights of the community, with read-only and read-write options.

mib-view —— The MIB View for the community to access.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add community public, and the community has read-write management right to View viewDefault:

Device(config)# snmp-server community public read-write viewDefault

53.6 snmp-server host

Description

The **snmp-server host** command is used to add Notification. To delete the corresponding Notification, please use **no snmp-server host** command.

Syntax

snmp-server host *ip udp-port user-name* [smode { v1 | v2c | v3 }] [slev { noAuthNoPriv | authNoPriv | authPriv }] [type { trap | inform }] [retries *retries*] [timeout *timeout*]

no snmp-server host *ip user-name*

Parameter

ip —— The IP Address of the management Host. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.100 or fe80::1234.

udp-port —— UDP port, which is used to send notifications. The UDP port functions with the IP address for the notification sending. It ranges from 1 to 65535.

user-name —— The User name of the management station.

smode —— The Security Model of the management station, with v1, v2c and v3 options. By default, the option is v1.

slev —— The Security Level of SNMP v3 User. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). By default, the Security Level is noAuthNoPriv.

type —— The type of the notifications, with trap and inform options. Trap indicates traps are sent, while inform indicates informs are sent. The inform type has a higher security than the trap type and resend and timeout need to be configured if you select this option. You can only select the trap type in Security Model v1. By default, the type of the notifications is "trap".

retries —— The amount of times the device retries an inform request, ranging from 1 to 255. The device will resend the inform request if it doesn't get the response from the management station during the Timeout interval, and it will terminate resending the inform request if the resending times reach the specified Retry times.

timeout —— The maximum time for the device to wait for the response from the management station before resending a request, ranging from 1 to 3600 in seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a Notification entry, and configure the IP address of the management Host as 192.168.0.146, the UDP port as 162, the User name of the management station as admin, the Security Model of the management station as v2c, the type of the notifications as inform, the maximum time for the device to wait as 1000 seconds, and the retries time as 100:

Device(config)# snmp-server host 192.168.0.146 162 admin **smode** v2c **type** inform **retries** 100 **timeout** 1000

Add a Notification entry, and configure the IP Address of the management Host as fe80::1234, the UDP port as 162, the User name of the management station as admin, the Security Model of the management station as v2c, the type of the notifications as inform, the maximum time for the device to wait as 1000 seconds, and the retries time as 100:

Device(config)# snmp-server host fe80::1234 162 admin **smode** v2c **type** inform **retries** 100 **timeout** 1000

53.7 snmp-server engineID

Description

The **snmp-server engineID** command is used to configure the local and remote engineID of the device. To restore to the default setting, please use **no snmp-server engineID** command.

Syntax

snmp-server engineID { [local *local-engineID*] [remote *remote-engineID*] }

no snmp-server engineID

Parameter

local-engineID —— Local Engine ID for local clients. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the device. Its length ranges from 10 to 64 hexadecimal characters, which must be even number meanwhile.

remote-engineID —— Remote Engine ID for the device. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the remote device which receives informs from the device. Its length ranges from 10 to 64 hexadecimal characters, which must be even number meanwhile. The **snmp-server engineID** will be disabled if the **local** and **remote** are both not configured.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Specify the local engineID as 1234567890, and the remote engineID as abcdef123456:

Device(config)# snmp-server engineID local 1234567890 **remote**

abcdef123456

53.8 snmp-server traps snmp

Description

The **snmp-server traps snmp** command is used to enable SNMP standard traps which include four types: linkup, linkdown, warmstart and coldstart. The command without parameter enables all SNMP standard traps. All SNMP standard traps are enabled by default. To disable the sending of SNMP standard traps, please use **no snmp-server traps snmp** command.

Syntax

snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

Parameter

linkup —— Indicates a port status changes from linkdown to linkup, and can be triggered when you connect a device to a port.

linkdown —— Indicates a port status changes from linkup to linkdown, and can be triggered when you disconnect a device to a port.

warmstart —— Indicates the SNMP feature on the device is reinitialized with the physical configuration unchanged. The trap can be triggered if you disable and then enable SNMP after the SNMP is completely configured and enabled.

coldstart —— Indicates an SNMP initialization caused by the reinitialization of the device system. The trap can be triggered when you reboot the device.

auth-failure —— Triggered when a received SNMP request fails the authentication.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP standard linkup trap for the device:

Device(config)# snmp-server traps snmp linkup

53.9 snmp-server traps

Description

The **snmp-server traps** command is used to enable SNMP extended traps. To disable the sending of SNMP extended traps, please use **no snmp-server traps** command. All SNMP extended traps are disabled by default.

Syntax

snmp-server traps { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory }

no snmp-server traps { bandwidth-control | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory }

Parameter

rate-limit ——Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.

cpu ——Monitors the load status of the device CPU. The trap can be triggered when the utilization rate of the CPU has exceeded the limit that you have set. The limit of CPU utilization rate for the device is 80% by default.

flash ——Triggered when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, and so on.

lldp remtableschange ——An lldp RemTablesChange notification is sent when the value of lldp StatsRemTableLastChangeTime changes. It can be utilized by an NMS host to trigger LLDP remote systems table maintenance polls.

lldp topologychange ——A notification generated by the local device to sense the change in the topology that indicates a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.

loopback-detection ——The feature is used to detect loopbacks. And the trap is disabled by default. The system will generate the trap when a loopback is detected or cleared.

storm-control ——The feature is used to monitor network storms. And the trap is disabled by default. The system will generate the trap when the rate of broadcast or multicast reaches the limit of storm control.

spanning-tree ——The feature is used to monitor the spanning tree status. And the trap is disabled by default. The system will generate the trap in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a packet with TC flag or a TCN packet.

memory ——The feature is used to monitor the memory. And the trap is disabled by default. The system will generate the trap when the memory utilization exceeds 80%.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP extended bandwidth-control trap for the device:

Device(config)# snmp-server traps bandwidth-control

53.10 snmp-server traps ddm

Note: This command is only available on certain devices.

Description

The **snmp-server traps ddm** command is used to enable the corresponding DDM traps. DDM function is used to monitor the status of the SFP modules inserted into the SFP ports on the device. The command without parameter enables all SNMP DDM traps. To disable the sending of SNMP DDM traps, use **no snmp-server traps ddm** command. All DDM traps are disabled by default.

Syntax

snmp-server traps ddm [temperature | voltage | bias_current | tx_power | rx_power]

no snmp-server traps ddm [temperature | voltage | bias_current | tx_power | rx_power]

Parameter

temperature ——Monitors the temperature of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold.

voltage ——Monitors the voltage of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold.

bias_current ——Monitors the bias current of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold.

tx_power ——Monitors the TX Power of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold.

rx_power ——Monitors the RX Power of SFP modules inserted into the SFP ports on the device. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold.

User guidelines

The **snmp-server traps ddm** command without any parameter is used to enable all the types of DDM traps. And the **no snmp-server traps ddm** command without any parameter is used to disable all the types of DDM traps.

For more instructions about the alarm threshold or warning threshold, refer to Chapter 11 DDM Commands.

Command Mode

Global Configuration Mode

Example

Enable all the SNMP DDM traps for the device:

```
Device(config)# snmp-server traps ddm
```

53.11 snmp-server traps vlan

Description

The **snmp-server traps vlan** command is used to enable the corresponding VLAN traps. The command without parameter enables all SNMP VLAN traps. To disable this function, please use **no snmp-server traps vlan** command. All VLAN traps are disabled by default.

Syntax

snmp-server traps vlan [create | delete]

no snmp-server traps vlan [create | delete]

Parameter

create ——Triggered when certain VLANs are created successfully.

delete ——Triggered when certain VLANs are deleted successfully.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all SNMP extended VLAN-related traps for the device:

```
Device(config)# snmp-server traps vlan
```

Enable VLAN-created trap only for the device:

```
Device(config)# snmp-server traps vlan create
```

53.12 snmp-server traps security

Description

The **snmp-server traps security** command is used to enable the corresponding security traps. To disable this feature, please use **no snmp-server traps security** command. All security traps are disabled by default.

Syntax

snmp-server traps security { dhcp-filter | ip-mac-binding | acl **}**

no snmp-server traps security { dhcp-filter | ip-mac-binding **}**

Parameter

dhcp-filter —— Triggered when the DHCPv4 Filter feature is enabled and the device receives DHCP packets from an illegal DHCP server.

ip-mac-binding —— Triggered when the ARP Inspection feature is enabled and the device receives an illegal ARP packet, or the IPv4 Source Guard feature is enabled and the device receives an illegal IP packet.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the DHCP filter trap for the device:

```
Device(config)# snmp-server traps security dhcp-filter
```

53.13 snmp-server traps acl

Description

The **snmp-server traps acl** command is used to enable the ACL trap. To disable this feature, please use **no snmp-server traps acl** command. It is disabled by default.

The trap monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in ACL rule settings enabled, the device will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

Syntax

snmp-server traps acl

no snmp-server traps acl

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the ACL trap for the device:

```
Device(config)# snmp-server traps acl
```

53.14 snmp-server traps ip

Description

The **snmp-server traps ip** command is used to enable IP traps. To disable this feature, please use **no snmp-server traps ip** command. All IP traps are disabled by default.

Syntax

snmp-server traps ip { change | duplicate }

no snmp-server traps ip { change | duplicate }

Parameter

change —— Enable SNMP IP change traps. The trap monitors the IP changed of each interface. The trap can be triggered when the IP address of any interface is changed.

duplicate —— Enable SNMP IP duplicate traps. The trap can be triggered when the device detects an IP conflict event.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the IP-Change trap for the device:

```
Device(config)# snmp-server traps ip change
```

53.15 snmp-server traps link-status

Description

The **snmp-server traps link-status** command is used to enable SNMP link status trap for the specified port. To disable the sending of SNMP link status trap, please use **no snmp-server traps link-status** command. By default, it is disabled.

Syntax

snmp-server traps link-status

no snmp-server traps link-status

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP link status trap for port 3:

```
Device(config)# interface gigabitEthernet 1/0/3
Device(config-if)# snmp-server traps link-status
```

53.16 rmon history

Description

The **rmon history** command is used to configure the history sample entry. To return to the default configuration, please use **no rmon history** command. RMON (Remote Monitoring), basing on SNMP architecture, functions to monitor the network. History Group is one of the commonly used RMON Groups. After a history group is configured, the device collects network statistics information periodically, based on which the management station can monitor network effectively.

Syntax

rmon history *index* **interface gigabitEthernet** *port* [interval *interval*] [owner *owner-name*] [buckets *number*]

no rmon history *index*

Parameter

index —— The index number of the entry, ranging from 1 to 12, in the format of 1-3,5.

port ——The Ethernet port number.

interval —— The interval to take samplings from the port, ranging from 10 to 3600 in seconds. By default, it is 1800.

owner-name —— The owner of the history sample entry, ranging from 1 to 16 characters. By default, it is "monitor".

number —— The maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 130. The default is 50 buckets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the sample port as Gi1/0/2 and the sample interval as 100 seconds for the entry 1-3:

```
Device(config)# rmon history 1-3 interface gigabitEthernet 1/0/2 interval
100 owner owner1
```

53.17 rmon event

Description

The **rmon event** command is used to configure the entries of SNMP-RMON Event. To return to the default configuration, please use **no rmon event** command. Event Group, as one of the commonly used RMON Groups, is used to define RMON events. Alarms occur when an event is detected.

Syntax

rmon event *index* [user *user-name*] [description *descript*] [type { none | log | notify | log-notify }] [owner *owner-name*]

no rmon event *index*

Parameter

index —— The index number of the event entry, ranging from 1 to 12. You can only select one entry for each command.

user-name —— The name of the User to which the event belongs, ranging from 1 to 16 characters. By default, it is "public".

descript —— The description of the event, ranging from 1 to 16 characters. By default, it is empty.

type —— The event type, with none, log, notify and both options. None indicates no processing, log indicates logging the event, notify indicates sending trap messages to the management station, and both indicates logging the event and sending trap messages to the management station.

owner-name —— The owner of the event entry, ranging from 1 to 16 characters. By default, it is "monitor".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the user name of entry 1, 2, 3 and 4 as user1, the description of the event as description1, the type of event as log and the owner of the event as owner1:

```
Device(config)# rmon event 1-4 user user1 description description1 type
log owner owner1
```

53.18 rmon alarm

Description

The **rmon alarm** command is used to configure SNMP-RMON Alarm Management. To return to the default configuration, please use **no rmon alarm** command. Alarm Group is one of the commonly used RMON Groups. RMON alarm management allows monitoring the specific alarm variables. When the value of a monitored variable exceeds the threshold, an alarm event is generated, which triggers the device to act in the set way.

Syntax

rmon alarm *index* { stats-index *sindex* } [alarm-variable { revbyte | revpkt | bpkt | mpkt | crc-lign | undersize | oversize | jabber | collision | 64 | 65-127 | 128-511 | 512-1023 | 1024-10240 }] [s-type { absolute | delta}] [rising-threshold *r-hold*] [rising-event-index *r-event*] [falling-threshold *f-hold*] [falling-event-index *f-event*] [a-type {rise | fall | all}] [owner *owner-name*] [interval *interval*]

no rmon alarm *index*

Parameter

index —— The index number of the Alarm Management entry, ranging from 1 to 12, in the format of 1-3,5.

sindex —— Specify the statistics index.

alarm-variable —— The alarm variable. By default, the option is revbyte.

s-type —— Sample Type, which is the sampling method for the selected variable and comparing the value against the thresholds. There are two options, absolute and delta. Absolute indicates comparing the values directly with the thresholds at the end of the sampling interval. Delta indicates subtracting the last sampled value from the current value, and then comparing the difference in the values with the threshold. By default, the Sample Type is absolute.

r-hold —— The rising counter value that triggers the Rising Threshold alarm, ranging from 1 to 2147483647. By default, it is 100.

r-event —— Rise Event, which is the index of the corresponding event which will be triggered if the sampled value is larger than the Rising Threshold. It ranges from 1 to 12.

f-hold —— The falling counter value that triggers the Falling Threshold alarm, ranging from 1 to 2147483647. By default, it is 100.

f-event —— Fall Event, which is the index of the corresponding event which will be triggered if the sampled value is lower than the Falling Threshold. It ranges from 1 to 12.

a-type —— Alarm Type, with rise, fall and all options. Rise indicates that the alarm event will be triggered when the sampled value exceeds the Rising Threshold, fall indicates that the alarm event will be triggered when the sampled value is under the Falling Threshold, and all indicates that the alarm event will be triggered either the sampled value exceeds the Rising Threshold or is under the Falling Threshold. By default, the Alarm Type is all.

owner-name —— The owner of the entry, ranging from 1 to 16 characters. By default, it is monitor.

interval —— The alarm interval time, ranging from 10 to 3600 in seconds. By default, it is 1800.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure rmon alarm entries 1-3 binding with statistics entry 2, the owners as owner1 and the alarm intervals as 100 seconds:

Device(config)#rmon alarm 1-3 **stats-index** 2 **owner** owner1 **interval** 100

53.19 rmon statistics

Description

The **rmon statistics** command is used to configure the entries of SNMP-RMON statistics. To delete the corresponding entry, please use **no rmon statistics** command. The maximum supported entries are 1000.

Syntax

rmon statistics *index* **interface gigabitEtherne**t *port* [owner *owner-name*] [status { underCreation | valid }]

no rmon statistics *index*

Parameter

index —— The index number of the statistics entry, ranging from 1 to 65535, in the format of 1-3,5.

port —— The statistics port number, in the format of 1/0/1.

owner-name —— The creator of the event entry, ranging from 1 to 16 characters. By default, it is "monitor".

status —— The status of the statistics entry, either "underCreation" or "valid". "underCreation" means this entry won't take effect until it is modified to "valid"; "valid" means this entry takes effect immediately after it is created.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the statistics entries 1-3 with the statistics port as 1/0/1, owner as owner1 and status as valid:

Device(config)#rmon statistics 1-3 **interface gigabitEthernet** 1/0/1 **owner** owner1 **status** valid

53.20 show snmp-server

Description

The **show snmp-server** command is used to display SNMP configuration globally.

Syntax

show snmp-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display SNMP configuration globally:

Device# show snmp-server

53.21 show snmp-server view

Description

The **show snmp-server view** command is used to display the View table.

Syntax

show snmp-server view

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the View table:

```
Device# show snmp-server view
```

53.22 show snmp-server group

Description

The **show snmp-server group** command is used to display the Group table.

Syntax

show snmp-server group

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Group table:

```
Device# show snmp-server group
```

53.23 show snmp-server user

Description

The **show snmp-server user** command is used to display the User table.

Syntax

show snmp-server user

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the User table:

```
Device# show snmp-server user
```

53.24 show snmp-server community

Description

The **show snmp-server community** command is used to display the Community table.

Syntax

show snmp-server community

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Community table:

```
Device# show snmp-server community
```

53.25 show snmp-server host

Description

The **show snmp-server host** command is used to display the Host table.

Syntax

show snmp-server host

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Host table:

```
Device# show snmp-server host
```

53.26 show snmp-server engineID

Description

The **show snmp-server engineID** command is used to display the engineID of the SNMP.

Syntax

show snmp-server engineID

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the engineID:

```
Device# show snmp-server engineID
```

53.27 show rmon history

Description

The **show rmon history** command is used to display the configuration of the history sample entry.

Syntax

show rmon history [*index*]

Parameter

index —— The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all history sample entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of all history sample entries:

```
Device# show rmon history
```

53.28 show rmon event

Description

The **show rmon event** command is used to display the configuration of SNMP-RMON Event.

Syntax

show rmon event [*index*]

Parameter

index —— The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all SNMP-RMON enabled entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Event configuration of entry1-4:

```
Device# show rmon event 1-4
```

53.29 show rmon alarm

Description

The **show rmon alarm** command is used to display the configuration of the Alarm Management entry.

Syntax

show rmon alarm [*index*]

Parameter

index —— The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all Alarm Management entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of the Alarm Management entry 1-2:

```
Device# show rmon alarm 1-2
```

53.30 show rmon statistics

Description

The **show rmon statistics** command is used to display the configuration of the specified statistics entry.

Syntax

show rmon statistics [*index*]

Parameter

index —— The index number of the statistics entry selected to display the configuration, ranging from 1 to 65535. By default, the configuration of all statistics entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of the statistics entry 1:

```
Device#show rmon statistics 1
```

Chapter 54 ND Detection Commands

The ND Detection feature allows the device to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configurations.

54.1 ipv6 nd detection

Description

The **ipv6 nd detection** command is used to enable the ND Detection function globally. To disable the ND Detection function, please use **no ipv6 nd detection** command.

Syntax

ipv6 nd detection

no ipv6 nd detection

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function globally:

```
Device(config)#ipv6 nd detection
```

54.2 ipv6 nd detection vlan

Description

The **ipv6 nd detection vlan** command is used to enable ND Detection function on a specified VLAN. To disable ND Detection function on this VLAN, please use **no ipv6 nd detection vlan** command.

Syntax

ipv6 nd detection vlan *vlan-range*

no ipv6 nd detection vlan *vlan-range*

Parameter

vlan-range ——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function on VLAN 1,4,6-7:

Device(config)#ipv6 nd detection vlan 1,4,6-7

54.3 ipv6 nd detection vlan logging

Description

The **ipv6 nd detection vlan logging** command is used to enable Log function on a specified VLAN. To disable Log function on this VLAN, please use **no ipv6 nd detection vlan logging** command.

Syntax

ipv6 nd detection vlan *vlan-range* **logging**

no ipv6 nd detection vlan *vlan-range* **logging**

Parameter

vlan-range ——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the Log function on VLAN 1,4,6-7:

Device(config)#ipv6 nd detection vlan 1,4,6-7 **logging**

54.4 ipv6 nd detection trust

Description

The **ipv6 nd detection trust** command is used to configure the port for which the ND Detection function is unnecessary as the Trusted Port. To clear the Trusted Port list, please use **no ipv6 nd detection trust** command .The specific port, such as up-linked port, routing port and LAG port, should be set

as Trusted Port. To ensure the normal communication of the device, please configure the ND Detection Trusted Port before enabling the ND Detection function.

Syntax

Ipv6 nd detection trust

no ipv6 nd detection trust

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet/ interface port-channel / interface range port-channel)

Example

Configure the Gigabit Ethernet ports 1/0/2-5 as the Trusted Port:

```
Device(config)#interface range gigabitEthernet 1/0/2-5
Device(config-if-range)#ipv6 nd detection trust
```

54.5 show ipv6 nd detection

Description

The **show ipv6 nd detection** command is used to display the ND detection global configuration including the enable/disable status.

Syntax

show ipv6 nd detection

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ND Detection configuration globally:

```
Device(config)#show ipv6 nd detection
```

54.6 show ipv6 nd detection interface

Description

The **show ipv6 nd detection interface** command is used to display the interface configuration of ND Detection.

Syntax

show ipv6 nd detection interface[fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]

Parameter

port——The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the configuration of Gigabit Ethernet port 1/0/1:

Device(config)#show ipv6 nd detection interface gigabitEthernet 1/0/1

Display the configuration of all Ethernet ports:

Device(config)#show ipv6 nd detection interface

54.7 show ipv6 nd detection statistics

 **Note:** This command is only available on certain devices.

Description

The **show ipv6 nd detection statistics** command is used to display the ND statistics of each VLAN, including the number of forwarded and dropped ND packets.

Syntax

show ipv6 nd detection statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ipv6 ND Detection statistics of each VLAN.

Device(config)#show ipv6 nd detection statistics

54.8 show ipv6 nd detection vlan

Description

The **show ipv6 nd detection vlan** command is used to display the VLAN configuration of ND Detection.

Syntax

show ipv6 nd detection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ipv6 ND Detection configuration of VLAN.

```
Device(config)#show ipv6 nd detection vlan
```

Chapter 55 System Log Commands

The log information will record the settings and operation of the device respectively for you to monitor operation status and diagnose malfunction.

55.1 logging buffer

Description

The **logging buffer** command is used to store the system log messages to an internal buffer. To disable the log buffer function, please use the **no logging buffer** command. Local Log is the system log information saved in the device. It has two output channels, that is, it can be saved to two different positions, log buffer and log flash memory. The log buffer indicates the RAM for saving system log and the information in the log buffer can be got by show logging buffer command. It will be lost when the device is restarted.

Syntax

logging buffer

no logging buffer

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the system log buffer:

```
Device(config)#logging buffer
```

55.2 logging buffer level

Description

The **logging buffer level** command is used to configure the severity level and the status of the configuration input to the log buffer. To return to the default configuration, please use **no logging buffer level** command.

Syntax

logging buffer level *level*

no logging buffer level

Parameter

level—— Severity level of the log information output to each channel. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output. By default, it is 6 indicating that the log information with level 0-6 will be saved in the log buffer.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the severity level as 5:

Device(config)#logging buffer level 5

55.3 logging file flash

Description

The **logging file flash** command is used to store the log messages in a file in the flash on the device. To disable the log file flash function, please use **no logging file flash** command. This function is disabled by default. The log file flash indicates the flash sector for saving system log. The information in the log file of the flash will not be lost after the device is restarted and can be got by the show logging flash command.

Syntax

logging file flash

no logging file flash

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the log file flash function:

```
Device(config)#logging file flash
```

55.4 logging file flash frequency

Description

The **logging file flash frequency** command is used to specify the frequency to synchronize the system log file in the log buffer to the flash. To resume the default synchronizing frequency, please use the **no logging file flash frequency** command.

Syntax

logging file flash frequency { periodic *periodic* | immediate }

no logging file flash frequency

Parameter

periodic —— The frequency to synchronize the system log file in the log buffer to the flash, ranging from 1 to 48 hours. By default, the synchronization process takes place every 24 hours.

immediate —— The system log file in the buffer will be synchronized to the flash immediately. This option will reduce the life of the flash and is not recommended.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify the log file synchronization frequency as 10 hours:

```
Device(config)#logging file flash frequency periodic 10
```

55.5 logging file flash level

Description

The **logging file flash level** command is used to specify the system log message severity level. Messages will a severity level equal to or higher than this value will be stored to the flash. To restore to the default level, please use **no logging file flash level** command.

Syntax

logging file flash level *level*

no logging file flash level

Parameter

level—— Severity level of the log message. There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be saved to the flash. By default, it is 3 indicating that the log message marked with 0–3 will be saved in the log flash.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Save the log messages with their severities equal or higher than 7 to the flash :

```
Device(config)#logging file flash level 7
```

55.6 logging host index

Description

The **logging host index** command is used to configure the Log Host. To clear the configuration of the specified Log Host, please use **no logging host index** command. Log Host is to receive the system log from other devices. You can remotely monitor the settings and operation status of other devices through the log host.

Syntax

logging host index *idx host-ip level*

no logging host index *idx*

Parameter

idx —— The index of the log host. The device supports 4 log hosts at most.

host-ip —— The IP for the log host.

level —— The severity level of the log information sent to each log host. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be sent to the corresponding log host. By default, it is 6 indicating that the log information marked with 0–6 will be sent to the log host.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable log host 2 and set its IP address as 192.168.0.148, the level 5:

Device(config)# logging host index 2 192.168.0.148 5

55.7 logging console

Description

The **logging console** command is used to send the system logs to the console port. To disable logging to the console, please use **no logging console** command. This function is enabled by default.

Syntax

logging console

no logging console

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable logging to the console port:

```
Device(config)# logging console
```

55.8 logging console level

Description

The **logging console level** command is used to limit messages logged to the console port. System logs no higher than the set threshold level will be displayed on the console port. To restore the threshold level to default value, please use **no logging console level** command.

Syntax

logging console level *level*

no logging monitor level

Parameter

level—— Severity level of the log information output to the console port. There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0–5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Output the log information with severity levels between 0–7 to the console port:

```
Device(config)# logging console level 7
```

55.9 logging monitor

Description

The **logging monitor** command is used to display the system logs on the terminal devices. To disable logging to the terminal, please use **no logging monitor** command. This function is enabled by default.

Syntax

logging monitor

no logging monitor

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Disable logging to the terminal devices:

```
Device(config)# no logging monitor
```

55.10 logging monitor level

Description

The **logging monitor level** command is used to limit messages logged to the terminal devices. System logs no higher than the set threshold level will be displayed on the terminal devices. To restore the threshold level to default value, please use **no logging monitor level** command.

Syntax

logging monitor level *level*

no logging monitor level

Parameter

level—— Severity level of the log information output to the terminal devices. There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will

be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0–5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Output the log information with severity levels between 0–7 to the terminal devices:

```
Device(config)# logging monitor level 7
```

55.11 clear logging

Description

The **clear logging** command is used to clear the information in the log buffer and log file.

Syntax

clear logging [buffer | flash]

Parameter

buffer | flash —The output channels: buffer and flash. Clear the information of the two channels, by default.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Clear the information in the log file:

```
Device(config)# clear logging buffer
```

55.12 show logging local-config

Description

The **show logging local-config** command is used to display the configuration of the Local Log output to the console, the terminal, the log buffer and the log file.

Syntax

show logging local-config

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the Local Log:

```
Device(config)# show logging local-config
```

55.13 show logging loghost

Description

The **show logging loghost** command is used to display the configuration of the log host.

Syntax

show logging loghost [*index*]

Parameter

index——The index of the log host whose configuration will be displayed, ranging from 1 to 4. Display the configuration of all the log hosts by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the log host 2:

```
Device(config)# show logging loghost 2
```

55.14 show logging buffer

Description

The **show logging buffer** command is used to display the log information in the log buffer according to the severity level.

Syntax

show logging buffer [level *level*]

Parameter

level—— Severity level. There are 8 severity levels marked with values 0–7. The information of levels with priority not lower than the select level will display. Display all the log information in the log buffer by default.

word—— Display log information containing specified word.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the log information from level 0 to level 5 in the log buffer:

```
Device(config)# show logging buffer level 5
```

55.15 show logging flash

Description

The **show logging flash** command is used to display the log information in the log file according to the severity level.

Syntax

show logging flash [level *level*]

Parameter

level —— Severity level. There are 8 severity levels marked with values 0–7. The information of levels with priority not lower than the select level will display. Display all the log information in the log file by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the log information with the level marked 0-3 in the log file:

```
Device(config)# show logging flash level 3
```

Chapter 56 ERPS Commands

ERPS (Ethernet Ring Protection Switching) is an Ethernet ring link layer technology with high reliability and stability. It can prevent broadcast storms caused by the data loop if the Ethernet ring is complete. With a high convergence speed, it can quickly restore the communication paths among the nodes in the ring network when a link failure happens.

56.1 erps ring

Description

The **erps ring** command is used to enable the ERPS ring function globally and create an ERPS ring. To disable the ERPS ring function, please use **no erps ring** command.

Syntax

erps ring *ring-id*

no erps ring *ring-id*

Parameter

ring-id —— The ID of the ERPS ring, ranging from 1 to 8.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ERPS ring function globally:

```
Device(config)#erps ring 1
```

56.2 control-vlan

Description

The **control-vlan** command is used to configure a control VLAN for an ERPS ring to forward RAPS PDUs .

Syntax

control-vlan *vlan-id*

Parameter

vlan-id—— Specify the ID of a control VLAN for ERPS ring, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure control VLAN 2 in ERPS ring 1:

```
Device(config)#erps ring 1
Device(ring-config)#control-vlan 2
```

56.3 description

Description

The **description** command is used to add description information of an ERPS ring.

Syntax

description *description*

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add description information “ring 1”:

```
Device(ring-config)#description “ring 1”
```

56.4 guard-timer

Description

The **guard-timer** command is used to configure the Guard timer in an ERPS ring. By default, the Guard timer is 200 centiseconds in an ERPS ring. To disable the guard-timer function, please use **no guard-timer** command.

Syntax

guard-timer *time*

no guard-timer

Parameter

time —— The time setting for guard-timer, ranging from 1 to 200, In centiseconds.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time for guard-timer as 100:

```
Device(ring-config)#guard-timer 100
```

56.5 wtr-timer

Description

The **wtr-timer** command is used to configure the Wait to Restore (WTR) timer in an ERPS ring. By default, the WTR timer is 5 minutes in an ERPS ring. To disable the wtr-timer function, please use **no wtr-timer** command.

Syntax

wtr-timer *time*

no wtr-timer

Parameter

time —— The time setting for wtr-timer, ranging from 1 to 12.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time for wtr-timer as 1:

```
Device(ring-config)#wtr-timer 1
```

56.6 holdoff-timer

Description

The **holdoff-timer** command is used to configure the Holdoff timer in an ERPS ring. By default, the Holdoff timer is 0 deciseconds in an ERPS ring. When a fault occurs, the fault is not immediately reported to ERPS. Instead, the Holdoff timer starts. If the fault persists after the timer expires, the fault will be reported to ERPS. To disable the holdoff-timer function, please use **no holdoff-timer** command.

Syntax

holdoff-timer *time*

no holdoff-timer

Parameter

time —— The time setting for holdoff-timer, ranging from 1 to 100.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the time for holdoff-timer as 10:

```
Device(ring-config)#holdoff-timer 10
```

56.7 protected-instance

Description

The **protected-instance** command is used to configure the Ethernet ring protection (ERP) instances in an ERPS ring. To disable the protected-instance function, please use **no protected-instance** command. By default, no ERP instance is configured in an ERPS ring.

Syntax

protected-instance *instance*

no protected-instance *instance*

Parameter

instance —— The protected instance for the ERPS ring, ranging from 1 to 8.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the protected instance as 1, and map VLAN10-20 to instance 1:

```
Device(ring)#spanning-tree mode mstp
Device(ring)#spanning-tree mst configuration
Device(ring)#instance 1 vlan 10-20
Device(ring-config)#protected-instance 1
```

56.8 raps-mel

Description

The **raps-mel** command is used to configure the value of the MEL field in Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs) of the ERPS ring. By default, the value of the MEL field in RAPS PDUs is 7.

Syntax

raps-mel *mel*

Parameter

mel—— MEL value of the ERPS ring, ranging from 0 to 7.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the MEL value as 1:

```
Device(ring-config)#raps-mel 1
```

56.9 revertive

Description

The **revertive** command is used to configure the revertive switching or non-revertive switching of the ERPS ring. To disable this function, please use the **revertive disable** command. By default, ERPS rings use revertive switching.

Syntax

revertive enable

revertive disable

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the revertive function:

```
Device(ring-config)#revertive enable
```

56.10 sub-ring

Description

The **sub-ring** command is used to configure the ERPS ring as an sub-ring. To disable this function, please use the **no sub-ring** command.

Syntax

sub-ring

no sub-ring

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the sub-ring function:

```
Device(ring-config)#sub-ring
```

56.11 tc-notify erps

Description

The **tc-notify erps** command is used to enable the network topology change notification function. To disable this function, please use the **no tc-notify erps** command. By default, this function is disabled.

Syntax

tc-notify erps ring *ring-id*

no tc-notify erps ring *ring-id*

Parameter

ring-id—— the ring ID of the notification, ranging from 1 to 8.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the network topology change notification function of ring 1:

```
Device(ring-config)#tc-notify erps ring 1
```

56.12 tc-protection interval

Description

The **tc-protection interval** command is used to configure the network topology change protection interval for sending topology change notification messages. To disable this function, please use the **no tc-protection interval** command.

Syntax

tc-protection interval *interval*

no tc-protection interval *interval*

Parameter

interval—— the time interval for tc-protection, ranging from 1 to 600.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the tc-protection interval of the ERPS ring as 1:

```
Device(ring-config)#tc-protection interval 1
```

56.13 tc-protection threshold

Description

The **tc-protection threshold** command is used to configure the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval. To disable this function, please use the **no tc-protection threshold** command.

Syntax

tc-protection threshold *threshold*

no tc-protection threshold

Parameter

threshold—— the threshold for tc-protection, ranging from 1 to 255.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the tc-protection threshold of the ERPS ring as 1:

```
Device(ring-config)#tc-protection threshold 1
```

56.14 version

Description

The **version** command is used to configure the ERPS version.

Syntax

version *version*

Parameter

version—— the version of the ERPS function, ranging from 1 to 2.

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the ERPS version as 2:

```
Device(ring-config)#version 2
```

56.15 virtual-channel

Description

The **virtual-channel** command is used to configure the virtual channel (VC) mode for RAPS PDU transmission in a sub-ring. To disable this function, please use the **no virtual-channel** command.

Syntax

virtual-channel

no virtual-channel

Command Mode

ERPS Ring Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the virtual-channel function:

```
Device(ring-config)#virtual-channel
```

56.16 erps ring rpl

Description

The **erps ring rpl** command is used to add a port to the ERPS ring and specify the role of the port. To remove the role of the port, please use the **no erps ring rpl** command.

Syntax

erps ring *ring id* [**rpl** *owner*|*neighbour*]

Parameter

ring id—— the ID of the ring that the port joins.

owner—— configure the role of the port as owner.

neighbour—— configure the role of the port as neighbour.

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the role of port 1/0/2 in ring 1 as owner:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)#erps ring 1 rpl owner
```

56.17 erps ring protect-switch

Description

The **erps ring protect-switch** command is used to configure a port blocking mode for the ERPS port.

Syntax

erps ring *ring id* [**protect-switch** *force*|*manual*]

Parameter

ring id—— the ID of the ERPS ring, ranging from 1-255.

force——block a port forcibly.

manual—— indicate the MS mode for blocking an ERPS port.

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the switch mode of port 1/0/2 in ring 1 as force:

```
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)#erps ring 1 protect-switch force
```

56.18 no erps ring ringid description

Description

The **no erps ring ringid description** command is used to restore the ERPS ring's description to the default ring.

Syntax

no erps ring *ringid* **description**

Parameter

ringid—— ERPS ring ID, e.g., 1, 5, 8

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Restore the ERPS ring's description to the default ring:

```
Device(config)# no erps ring 1 description
```

56.19 no erps ring ringid raps-mel

Description

The **no erps ring ringid raps-mel** command is used to restore the ERPS ring's RAPS-MEL to the default value of 7.

Syntax

no erps ring *ringid* **raps-mel**

Parameter

ringid—— ERPS ring ID, e.g., 1, 5, 8

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Restore the ERPS ring's RAPS-MEL to the default value:

```
Device(config)# no erps ring 1 raps-mel
```

56.20 no erps ring ringid version

Description

The **no erps ring ringid version** command is used to restore the ERPS ring's version to the default value of 1.

Syntax

no erps ring *ringid* **version**

Parameter

ringid—— ERPS ring ID, e.g., 1, 5, 8

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Restore the ERPS ring's version to the default value of 1.:

```
Device(config)# no erps ring 1 version
```

56.21 show erps ring

Description

The **show erps ring** command is used to display the ERPS ring information.

Syntax

show erps ring {*ring-id* | *all*}

Parameter

ring id—— show the information of a specified ring, ranging from 1 to 8.

all—— show the information of all rings.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Show the information of all rings:

```
Device(config)#show erps ring all
```

56.22 show erps statistics

Description

The **show erps statistics** command is used to display the ERPS packet statistics.

Syntax

show erps statistics

show erps statistics ring *ringId*

Parameter

ringId—— ERPS ring ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display packet statistics for all ERPS rings:

```
Device(config)# show erps statistics
```

Display packet statistics for ERPS ring 1:

```
Device(config)# show erps statistics ring 1
```

Chapter 57 IS-IS Configuration Commands

Intermediate System to Intermediate System (IS-IS) is a dynamic routing protocol proposed by ISO. Currently, IS-IS is also supported in TCP/IP environments. It is a widely used protocol in Interior Gateway Protocols (IGP).

IS-IS is a link-state protocol, and the core concept of its routing calculation is the Shortest Path First (SPF) algorithm.

57.1 router isis

Description

The **router isis** command is used to create an IS-IS instance and enter the Router configuration mode. When the command includes a VRF name, it means that the IS-IS instance belongs to the VRF instance. When the VRF parameter is not specified, the IS-IS instance belongs to the public network. To delete the IS-IS instance, please use the **no router isis** command. When the VRFparameter is not specified, the corresponding instance will be deleted according to the area-tag.

Syntax

router isis *area-tag* [**vrf** *vrf-name*]
no router isis *area-tag* [**vrf** *vrf-name*]

Parameter

area-tag —— IS-IS instance name, used to identify an IS-IS instance on this switch.

vrf-name —— VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an ISIS instance aaa and add it to vrf1.

```
Device(config)# router isis aaa vrf vrf1
```

57.2 area-password

Description

The **area-password** command is used to enable the IS-IS Level-1 area authentication function. After the function is enabled, IS-IS will carry authentication information in the message exchange in the area and verify the authentication information. To disable this function, please use the **no area-password** command.

Syntax

area-password { **clear** | **md5** } { **0** | **7** } *text*

no area-password

Parameter

clear —— Encrypt in plain text.

md5 —— Encrypt using md5 algorithm.

0 —— Enter plain text.

7 —— Enter in cipher text.

text —— Password text

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure MD5 encrypted authentication for the IS-IS Level-1 area:

Device(config-router)#area-password md5 0 tp-link

57.3 domain-password

Description

This command is used to enable the authentication function of the IS-IS Level-2 area. After enabling this function, IS-IS will carry authentication information in the message exchange in this area and verify the

authentication information. To disable this function, please use the **no domain-password** command.

Syntax

domain-password { **clear** | **md5** } { **0** | **7** } *text*

no domain-password

Parameter

clear —— Encrypt in plain text.

md5 —— Encrypt using md5 algorithm.

0 —— Enter plain text.

7 —— Enter in cipher text.

text —— Password text

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure MD5 encrypted authentication for the IS-IS Level-2 area:

Device(config-router)#domain-password md5 0 *tp-link*

57.4 graceful-restart

Description

This command is used to enable the IS-IS Graceful Restart function. When enabled, IS-IS will send restart notification messages to neighboring routers before initiating a restart. During the restart process, IS-IS strives to preserve routing information to minimize impact on other devices in the network. To disable this function, please use the **no graceful-restart** command.

Syntax

graceful-restart

no graceful-restart

graceful-restart suppress-sa

no graceful-restart suppress-sa

graceful-restart t2-interval *t2-interval*

no graceful-restart t2-interval

graceful-restart t3-interval *t3-interval*

no graceful-restart t3-interval

Parameter

suppress-sa —— Suppress partial advertisement information during the IS-IS graceful restart process.

t2-interval —— The duration in IS-IS graceful restart during which the restarting router waits for neighboring routers to send CSNP (Complete Sequence Number PDU) to facilitate rapid database synchronization. The range is 30 to 1800 seconds, and the default value is 60 seconds.

T3-interval —— The duration in IS-IS graceful restart during which the restarting router waits for neighboring routers to acknowledge its graceful restart. The range is 30 to 1800 seconds, and the default value is 300 seconds.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure graceful restart for IS-IS routes:

```
Device(config-router)#graceful-restart

Device(config-router)#graceful-restart suppress-sa
```

57.5 hostname

Description

This command is used to enable the dynamic host name function of IS-IS. After enabling this function, IS-IS will configure a dynamic host name for the IS-IS system on the local switch and notify the neighbor device through the LSP message. To disable this function, please use the **no hostname** command.

Syntax

hostname { *name* | dynamic }

no hostname

Parameter

name —— Specified host name, in text form.

dynamic —— Use dynamic host name, in this mode, the system configured host name will be obtained.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the dynamic host name function of IS-IS:

```
Device(config-router)# hostname dynamic
```

57.6 is-type

Description

This command is used to set the IS area type, which is Level-1-2 by default. To restore the default configuration, please use the **no is-type** command.

Syntax

is-type { **level-1** | **level-1-2** | **level-2-only** }

no is-type

Parameter

level-1 —— Set the IS-IS area type to Level-1

level-1-2 —— Set the IS-IS area types to Level-1 and Level-2 level-2-only: Set the IS-IS area type to Level-2

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS area type to Level-1:

```
Device(config-router)# is-type level-1
```

57.7 log-adjacency-changes

Description

This command is used to enable S-IS to record events of adjacency state changes. To disable this function, please use the **no log-adjacency-changes** command.

Syntax

log-adjacency-changes

no log-adjacency-changes

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS area type to Level-1:

```
Device(config-router)# log-adjacency-changes
```

57.8 lsp-gen-interval

Description

This command is used to configure the interval for generating LSPs. When the local network flaps, the IS-IS local LSP may be frequently refreshed, causing frequent IS-IS flapping. To restore the default configuration, please use the **no lsp-gen-interval** command.

Syntax

lsp-gen-interval *interval*

no lsp-gen-interval

Parameter

interval—— The interval for generating LSPs, ranging from 1 to 120s. It is 30s by default.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the LSP generating interval to 10s:

```
Device(config-router)# lsp-gen-interval 10
```

57.9 lsp-mtu

Description

This command is used to configure the maximum length of a self-generated LSP. To restore the default configuration, please use the **no lsp-mtu** command.

Syntax

lsp-mtu *size*

no lsp-mtu

Parameter

size—— The maximum length of LSP, ranging from 512 to 4352 bytes. It is 1497 bytes by default.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the maximum length of LSP to 1024 bytes:

```
Device(config-router)# lsp-mtu 1024
```

57.10 lsp-refresh-interval

Description

This command is used to configure the interval for refreshing the IS-IS LSP. To restore the default configuration, please use the **no lsp-refresh-interval** command.

Syntax

lsp-refresh-interval *interval* [level-1 | level-2]

no lsp-refresh-interval

Parameter

interval —— The interval for refreshing the IS-IS LSP, ranging from 1 to 65535s. It is 900s by default.

level-1 —— LSP level-1 refresh interval

level-2 —— LSP level-2 refresh interval

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the LSP refresh interval to 100s:

```
Device(config-router)# lsp-refresh-interval 100
```

57.11 max-lsp-lifetime

Description

This command is used to configure the maximum lifetime of an IS-IS LSP packet. To restore the default configuration, please use the **no max-lsp-lifetime** command.

Syntax

max-lsp-lifetime *time* [level-1 | level-2]

no max-lsp-lifetime

Parameter

time —— The max lifetime of LSP, ranging from 350 to 65535s. It is 1200s by default.

level-1 —— LSP level-1 refresh interval

level-2 —— LSP level-2 refresh interval

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the maximum lifetime of an LSP to 1000s:

```
Device(config-router)# max-lsp-lifetime 1000
```

57.12 metric-style

Description

This command is used to configure IS-IS metric style. To restore the default configuration, please use the **no metric-style** command.

Syntax

metric-style { **narrow** | **transition** | **wide** }

no metric-style

Parameter

narrow —— Narrow mode. It is the default mode.

transition —— Compatible mode, supporting both narrow and wide modes.

wide —— Wide mode, mainly used for TE scenarios.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set IS-IS metric style to wide:

```
Device(config-router)# metric-style wide
```

57.13 net

Description

This command is used to configure NET of IS-IS. To delete NET, please use the **no net** command.

Syntax

net *net-name*

no net *net-name*

Parameter

net-name —— Network Entity Title, in the format of X...X.XXXX.XXXX.XXXX.00. The first "X...X" is the IS-IS area address, the 12 "X"s in the middle are the switch's System ID, and the last "00" is the SEL.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure IS-IS NET as 10.0000.0000.0000.1111.00:

```
Device(config-router)#net 10.0000.0000.0000.1111.00
```

57.14 purge-originator

Description

This command is used to enable the purge originator of IS-IS. To disable this function, please use the **no purge-originator** command.

Syntax

purge-originator

no purge-originator

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the purge originator of IS-IS:

```
Device(config-router)#purge-originator
```

57.15 set-attached-bit

Description

This command is used to set the ATT bit of IS-IS LSP. By default, Level-1-2 devices will set the ATT bit according to the rules of IS-IS protocol. After this command is configured, the ATT bit will always be set in Level-1 LSP. To cancel the setting of ATT bit, please use the **no set-attached-bit** command.

Syntax

set-attached-bit

no set-attached-bit

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the ATT bit of IS-IS LSP:

```
Device(config-router)#set-attached-bit
```

57.16 set-overload-bit

Description

This command is used to set the overload bit in IS-IS LSP. To cancel the overload bit setting, please use the **no set-overload-bit** command.

Syntax

set-overload-bit

no set-overload-bit

Parameter

None

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the overload bit in IS-IS LSP:

```
Switch(config-router)#set-overload-bit
```

57.17 spf interval

Description

This command is used to configure the frequency of SPF calculations in IS-IS to balance network convergence speed and CPU load. To restore the default settings, please use the **no spf-interval** command.

Syntax

spf-interval *time*

no spf-interva

Parameter

time —— The interval for SPF calculation. The range is 1 to 120 seconds, and the default value is 2 seconds

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the interval for SPF calculation to 5 seconds:

```
Device(config-router)# spf-interval 5
```

57.18 topology

Description

This command is used to enable global IS-IS network multi-topology, allowing independent logical topologies to be created for different protocols or services. To disable this configuration, please use the **no topology** command.

Syntax

topology { ipv6-unicast } [overload]

no topology { ipv6-unicast }

Parameter

ipv6-unicast —— IS-IS enables IPv6 unicast topology.

overload —— IS-IS enables topology to set overload bit.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure IS-IS multi-topology:

```
Device(config-router)#topology ipv6-unicast overload
```

57.19 clear isis neighbor

Description

This command is used to clear the neighbor relationship established by IS-IS and re-establish the relationship with neighbor device.

Syntax

clear isis neighbor [*system-id*]

Parameter

system-id: System ID of the specified neighbor.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear all IS-IS neighbors:

```
Device(config-router)#clear isis neighbor
```

57.20 redistribute

Description

This command is used to redistribute routes. In a multi-protocol deployment scenario, routes of other protocols or other IS-IS instances can be redistributed to IS-IS, which will then flood the routes throughout the entire area.

Syntax

redistribute { ipv4 { bgp | connected | rip | static | ospf *process-id* **| isis** *area-name* **} | ipv6 { bgp | connected | ospf6 | ripng | static } } { level-1 | level-2 }**

Parameter

ipv4 —— Redistribute IPv4 routing.

ipv6 —— Redistribute IPv6 routing.

bgp —— Redistribute BGP routing.

connected —— Redistribute direct routing.

ospf —— redirect OSPF routing.

process-id —— redirect OSPF routing instance number

isis —— redirect IS-IS routing

area-name —— redirect IS-IS routing area name

rip —— redirect RIP routing

static —— Redistribute static routes.

ospf6 —— Redistribute OSPFv3 routes.

ripng —— Redistribute RIPng routes.

level-1 —— Redirect to level-1 area.

level-2 —— Redirect to level-2 area.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Redistribute IPv4 BGP routes to the level-1 area of IS-IS:

```
Device(config-router)# redistribute ipv4 bgp level-1
```

57.21 distance

Description

This command is used to configure the distance of IS-IS protocol routes, that is, the route priority of IS-IS protocol. This function can change the priority strategy of different protocol routes in multi-protocol scenarios.

Syntax

distance *value*

Parameter

value —— Distance value, ranging from 1 to 255, and the default value is 110.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the distance of the IS-IS protocol to 100:

Device(config-router)#distance 100

57.22 ip router isis

Description

This command is used to enable IPv4 IS-IS on an interface, while its no form disables the IPv4 IS-IS functionality under the interface. Configuration of IS-IS settings under an interface is only permitted when either IPv4 or IPv6 IS-IS has been enabled. If both IPv4 and IPv6 IS-IS are disabled simultaneously, all IS-IS configurations under the interface will be cleared.

Syntax

ip router isis *area-name*

no ip router isis

Parameter

area-name —— Specify the area name of the IS-IS instance.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable interface VLAN 1 on IS-IS instance 1:

Device(config)#interface vlan 1

Device(config-if)#ip router isis 1

57.23 ipv6 router isis

Description

This command is used to enable IPv6 IS-IS on an interface. Its "no" form disables IPv6 IS-IS functionality on the interface. Interface-specific IS-IS configurations can only be performed when either IPv4 or IPv6 IS-IS is enabled. When both IPv4 and IPv6 IS-IS functionalities are disabled, all IS-IS configurations under the interface will be cleared.

Syntax

Ipv6 router isis *area-name*

no ipv6 router isis

Parameter

area-name —— Specify the area name of the IS-IS instance.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable interface VLAN 1 on IS-IS IPV6 instance 1:

```
Device(config)#interface vlan 1
Device(config-if)#ipv6 router isis 1
```

57.24 isis bfd

Description

This command is used to enable BFD on an interface and notify IS-IS. IS-IS can quickly detect changes in interface status. To disable this function, please use the no isis bfd command.

Syntax

isis bfd [*bfd-template*]

no isis bfd

Parameter

bfd-template —— BFD template name, depending on the global BFD template configuration

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable BFD on interface VLAN 1 and notify IS-IS:

```
Device(config)#interface vlan 1
Device(config-if)#isis bfd
```

57.25 isis circuit-type

Description

This command is used to configure the IS-IS area type of the interface. By default, the area type of the IS-IS interface is the area type configured globally for IS-IS. To restore the default configuration, please use the **no isis circuit-type** command.

Syntax

isis circuit-type { **level-1** | **level-1-2** | **level-2-only** }

no isis circuit-type

Parameter

level-1 —— Set the IS-IS area type to Level-1

level-1-2 —— Set the IS-IS area types to Level-1 and Level-2

level-2-only —— Set the IS-IS area type to Level-2

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS area type of interface VLAN 1 to Level-1:

Device(config)#interface vlan 1

Device(config-if)#isis circuit-type level-1

57.26 isis csnp-interval

Description

This command is used to configure the interval for sending CSNP packets of IS-IS on the interface. To restore the default configuration, please use the **no isis csnp-interval** command.

Syntax

isis csnp-interval *interval*

no isis csnp-interval

Parameter

interval—— The interval for sending CSNP packets, ranging from 1 to 600s, and the default value is 10.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the CSNP message sending interval of IS-IS on interface VLAN 1 to 20s:

Device(config)#interface vlan 1

Device(config-if)#isis csnp-interval 20

57.27 isis hello-interval

Description

This command is used to configure the interval for sending Hello packets of IS-IS on the interface. To restore the default configuration, please use the **no isis csnp-interval** command.

Syntax

isis hello-interval *interval*

no isis hello-interval

Parameter

interval—— The interval for sending Hello packets, ranging from 1 to 600s, and the default value is 3.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the Hello message sending interval of IS-IS on interface VLAN 1 to 10s:

```
Device(config)#interface vlan 1
Device(config-if)#isis hello-interval 10
```

57.28 isis hello-multiplier

Description

This command is used to configure the multiplier of the IS-IS Hello message on the interface. Hello-interval * Hello-multiplier is the neighbor's Hold timer. To restore the default configuration, please use the **no isis hello-multiplier** command.

Syntax

isis hello-multiplier *value*

no isis hello-multiplier

Parameter

value—— Hello multiplier, ranging from 2 to 100. It is 10 by default.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS Hello multiplier on interface VLAN 1 to 20:

Device(config)#interface vlan 1

Device(config-if)# isis hello-multiplier 20

57.29 isis metric

Description

This command is used to configure the IS-IS metric on the interface. To restore the default configuration, please use the **no isis metric** command.

Syntax

isis metric *value*

no isis metric

Parameter

value —— IS-IS metric, ranging from 0 to16777215. It is 10 by default.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS metric on interface VLAN 1 to 20:

Device(config)#interface vlan 1

Device(config-if)#isis metric 20

57.30 isis network point-to-point

Description

This command is used to configure the IS-IS network type of the interface. To restore the default configuration, please use the **no isis network point-to-point** command.

Syntax

isis network point-to-point

no isis network point-to-point

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS network type of interface VLAN 1 to P2P:

```
Device(config)#interface vlan 1
Device(config-if)# isis network point-to-point
```

57.31 isis passive

Description

This command is used to configure the IS-IS silent function on the interface. After it is enabled, the interface will not be able to perform IS-IS message exchange and route calculation. To disable this dunction, please use the **no isis passive** command.

Syntax

isis passive

no isis passive

Parameter

None.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Make the IS-IS on VALN 1 silent:

Device(config)#interface vlan 1

Device(config-if)#isis passive

57.32 isis password-key

Description

This command is used to enable the IS-IS authentication function. After the function is enabled, IS-IS will carry authentication information in the message exchange in the area and verify the authentication information. To disable this function, please use the **no area-password** command.

Syntax

isis password-key {**clear** | **md5**}{**0** | **7**} *text*

no isis password-key

Parameter

clear —— Encrypt in plain text.

md5 —— Encrypt using md5 algorithm.

0 —— Enter plain text.

7 —— Enter in cipher text.

text —— Password text

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure MD5 encrypted authentication for the IS-IS on VLAN 1:

Device(config)#interface vlan 1

Device(config-if)#isis password-ket md5 0 tp-link

57.33 isis priority

Description

This command is used to enable the IS-IS authentication function. After the function is enabled, IS-IS will carry authentication information in the message

exchange in the area and verify the authentication information. To disable this function, please use the **no area-password** command.

Syntax

isis priority *value*

no isis priority

Parameter

Value —— The DIS election priority of the interface, ranging from 0 to 127, and the default value is 64.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Set the IS-IS priority of interface VLAN 1 to 100:

```
Device(config)#interface vlan 1
Device(config-if)# isis priority 100
```

57.34 topology

Description

This command is used to enable IS-IS multi-topology under the interface, allowing the creation of independent logical topologies for different protocols or services. To disable this configuration, please use the **no topology** command.

Syntax

topology { ipv6-unicast }

no topology { ipv6-unicast }

Parameter

ipv6-unicast —— IS-IS enabled for IPv6 unicast topology.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure IS-IS multi-topology:

```
Device(config)#interface vlan 1
Device(config-if)#topology ipv6-unicast
```

57.35 isis three-way-handshake

Description

This command is used to configure the three-way handshake mechanism of the IS-IS neighbor on the interface. By default, IS-IS neighbor establishment is a two-way handshake mechanism. Two-way handshakes have the problem of one-way neighbor establishment. It is recommended to use the three-way handshake mechanism. To restore the default configuration, please use the **no isis three-way-handshake** command.

Syntax

isis three-way-handshake

no isis three-way-handshake

Parameter

None

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the IS-IS three-way handshake neighbor establishment mechanism on interface VLAN 1:

```
Device(config)#interface vlan 1
Device(config-if)#isis three-way-handshake
```

57.36 show isis database

Description

This command is used to view the IS-IS database information.

Syntax

show isis [tag { *area-name* } **] database [** *lsp-id* **| detail]**

Parameter

area-name —— Specify the IS-IS area name for the query.

lsp-id —— Specify the LSP ID for the query.

detail —— View detailed information

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the brief information of IS-IS database:

```
Device#show isis database
```

57.37 show isis graceful-restart

Description

This command is used to view the Graceful Restart information for IS-IS.

Syntax

show isis [tag { *area-name* } **] graceful-restart status**

Parameter

area-name —— Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS Graceful Restart information:

```
Device#show isis database
```

57.38 show isis hostname

Description

This command is used to view the IS-IS host name mapping information.

Syntax

show isis [tag { *area-name* }] hostname

Parameter

area-name —— Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS host name mapping information:

```
Device# show isis hostname
```

57.39 show isis neighbor

Description

This command is used to view the IS-IS neighbor information.

Syntax

show isis [tag { *area-name* **}] neighbor** [*system-id* | detail]

Parameter

area-name —— Specify the IS-IS area name for the query.

system-id —— Specify the neighbor's system ID for the query.

detail —— View detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the brief information of IS-IS neighbor:

```
Device# show isis neighbor
```

57.40 show isis route

Description

This command is used to view the IS-IS routing information.

Syntax

show isis [tag { *area-name* }] route

Parameter

None

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None**Example**

View the IS-IS routing information:

```
Device# show isis route
```

57.41 show isis summary

Description

This command is used to view the IS-IS summary.

Syntax

show isis [tag { *area-name* }] summary

Parameter

area-name —— Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS summary:

```
Device# show isis summary
```

57.42 show isis interface

Description

This command is used to view the IS-IS interface information.

Syntax

show isis [tag { *area-name* **}] interface [fastEthernet | gigabitEthernet | hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan] [detail]**

Parameter

area-name —— Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS interface information:

```
Device# show isis interface
```

57.43 show isis topology

Description

This command is used to view the IS-IS topology information.

Syntax

show isis [tag { *area-name* **}] topology [** level-1 | level-2 **]**

Parameter

area-name —— Specify the IS-IS area name for the query.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

View the IS-IS topology information:

```
Device# show isis topology
```

Chapter 58 RIP Configuration Commands

RIP (Routing Information Protocol) is a routing protocol suitable for small networks and has lower requirements in terms of bandwidth, configuration, and management. As a routing protocol based on distance vector algorithm, RIP uses hop count as the measurement standard.

58.1 router rip

Description

This **router rip** command is used to enable the RIP function on the switch. To disable this function, please use the **no router rip** command. You can specify to create a RIP instance under a certain VRF.

Syntax

router rip [**vrf** *vrf-name*]

no router rip [**vrf** *vrf-name*]

Parameter

vrf-name —— VRF instance name

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the RIP function of the switch in VRF v1:

```
Device(config)#router rip vrf v1
```

58.2 network

Description

The **network** command is used to enable the RIP function on the corresponding interface of the configured network segment. To disable the RIP function on the corresponding interface, please use **no network** command.

Syntax

network *network number*

no network *network number*

Parameter

network number —— Network number, the format is 192.168.0.0. If you enter an IP address, the network number will be automatically obtained based on the mask length of the natural network segment. Entering 0.0.0.0 means enabling the RIP function on all interfaces.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the rip function of network segment 192.168.0.0:

```
Device(config-router)#network 192.168.0.0
```

58.3 version

Description

The **version** command is used to configure the version of packets sent and received by RIP. By default, the switch sends RIPv2 packets and receives RIPv1 and RIPv2 packets. To restore the default message version settings, please use the **no version** command.

Syntax

version {1|2}

no version

Parameter

1 —— Send and receive RIPv1 messages.

2 —— Send and receive RIPv2 messages.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the RIP message version as RIPv1:

```
Device(config-router)#version 1
```

58.4 timer basic

Description

The **timer basic** command is used to configure the RIP timer. To restore the timer configuration to its default, please use the **no timer basic** command.

Syntax

timer basic *update-value timeout-value garbage-collect-value*

no timer basic

Parameter

update-value —— Routing table update time, ranging from 5 to 86400 seconds. The default value is 30.

timeout-value —— Routing table aging time, ranging from 5 to 86400 seconds. The default value is 180.

garbage-collect-value —— The expiration time after the routing entry is unreachable. When the entry is unreachable, the routing entry is removed from the routing table after the expiration time. The range is 5~86400 seconds, and the default value is 120.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the routing table update time to 50 seconds, the routing table aging time to 100 seconds, and the routing entry expiration time to 100 seconds:

```
Device(config-router)#timer basic 50 100 100
```

58.5 distance

Description

The **distance** command is used to configure the management distance of RIP routing. To restore the default configuration, please use the **no distance** command.

Syntax

distance *distance*

no distance

Parameter

distance —— Management distance of RIP routing, ranging from 1 to 255. The default value is 120.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the management distance of RIP routing to100:

```
Device(config-router)#distance 100
```

58.6 auto-summary

Description

The **auto-summary** command is used to enable the automatic summary function of RIP. After this function is enabled, routing entries will be automatically summarized into natural network segments, which can reduce the number of routing entries issued for each update. To disable this function, use the **no auto-summary** command.

Syntax

auto-summary

no auto-summary

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the automatic summary function of RIP:

```
Device(config-router)#auto-summary
```

58.7 default-metric

Description

The **default-metric** command is used to set the default metric for redirection routes. To restore the default configuration, please use the **no default-metric** command.

Syntax

default-metric *metric*

no default-metric

Parameter

metric —— The default metric of the redirect route, ranging from 1 to 15, and the default value is 1.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the default metric for redirection routes to 5:

```
Device(config-router)#default-metric 5
```

58.8 redistribute

Description

The **redistribute** command is used to set the metric for redirection routes. To restore the default configuration, please use the **no redistribute** command.

Syntax

redistribute { ospf *process-id* | connected | static } [**metric** *metric-value*]

no redistribute { ospf *process-id* | connected | static } [**metric**]

Parameter

ospf —— Enable RIP redirect OSPF routing function.

process-id —— Redirected OSPF process number.

connected —— Enable RIP redirect direct routing function.

static —— Enable RIP redirect static routing function.

metric-value —— The metric of the redirect route.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set RIP to redirect ospf process 1, and set metric to 3:

Device(config-router)#redistribute ospf 1 **metric** 3

58.9 allow-ecmp

Description

The **allow-ecmp** command is used to enable the ECMP function. To disable this function, please use the **no allow-ecmp** command.

Syntax

allow-ecmp

no allow-ecmp

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the ECMP function of RIP:

Device(config-router)#allow-ecmp

58.10 default-information originate

Description

The **default-information originate** command is used to introduce a default route into RIP. To disable this function, please use the **no default-information originate** command.

Syntax

default-information originate

no default-information originate

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Introduce a default route into RIP:

```
Device(config-router)#default-information originate
```

58.11 neighbor

Description

The **neighbor** command is used to configure the neighbor of RIP. After configuring the neighbor, RIP will send RIP packets to the neighbor through unicast packets. To clear the neighbor configuration, please use the **no neighbor** command.

Syntax

neighbor *ip-address*

no neighbor *ip-address*

Parameter

ip-address —— IP address of RIP's neighbor.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Specify 192.168.0.100 as the RIP neighbor:

```
Device(config-router)#neighbor 192.168.0.100
```

58.12 passive-interface

Description

The **passive-interface** command is used to configure the interface not to send RIP packets but only to receive RIP packets. A unicast response will be sent out when a neighbor is configured at the same time.To disable this function, please use the **no passive-interface** command.

Syntax

passive-interface interface { fastEthernet | gigabitEthernet | hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } *interface-value*

no passive-interface interface { fastEthernet | gigabitEthernet | hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } *interface-value*

Parameter

interface-value —— Specify the interface to be configured as passive-interface.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure VLAN 2 as passive-interface:

```
Device(config-router)# passive-interface interface vlan 2
```

58.13 ip rip authentication mode

Description

The **ip rip authentication mode** command is used to configure the authentication mode of RIP messages, and its no command is used to clear

the configuration of authentication mode. The authentication function only takes effect when the authentication mode and password are configured.

Syntax

ip rip authentication mode { md5 | simple }

no ip rip authentication mode

Parameter

md5 —— Configure the authentication mode of RIP to md5 authentication.

simple —— Configure the authentication mode of RIP to plain text authentication.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the RIP authentication mode of VLAN 2 to md5 authentication:

Device(config)#interface vlan 2

Device(config-if)#ip rip authentication mode md5

58.14 ip rip authentication string

Description

The **ip rip authentication string** command is used to configure the password and key ID for RIP authentication. The key ID is only used for md5 authentication.This command cannot be configured at the same time as the ip rip authentication key-chain command. To clear the password and key ID of RIP authentication, please use the **no ip rip authentication string** command.

Syntax

ip rip authentication string *password* **[key-id** *key-id-value* **]**

no ip rip authentication string

Parameter

password —— RIP authentication password, 16 characters at most.

key-id-value —— Key ID for RIP authentication, ranging from 1 to 255. The default value is 1.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the rip authentication password of interface VLAN 2 as tplink and the key ID as 2:

Device(config)#interface vlan 2

Device(config-if)#ip rip authentication string tplink **key-id 2**

58.15 ip rip authentication key-chain

Description

The **ip rip authentication key-chain** command is used to configure the password and key ID for RIP authentication by binding key-chain. This command cannot be configured at the same time as the ip rip authentication string command. To clear key-chain binding, please use the **no ip rip authentication key-chain** command.

Syntax

ip rip authentication key-chain *key-chain-name*

no ip rip authentication key-chain

Parameter

key-chain-name —— The name of the key-chain to be bound.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure key chain as 1, set key as 0, the corresponding password as tplink, and bind the RIP authentication of VLAN 1 to key chain 1:

Device(config)#key chain 1

Device (config-keychain)#key 0 key-string tplink

Device (config-keychain)#exit

```
Device (config)#interface vlan 1
Device (config-if)#ip rip authentication key-chain 1
```

58.16 ip rip receive version

Description

The **ip rip receive version** command is used to configure the version of RIP packets received by the interface. If the receive version of an interface is not configured, it will be determined by the global configuration. To restore the default configuration, please use the **no ip rip receive version** command.

Syntax

ip rip receive version { 1 | 2 }

no ip rip receive version

Parameter

1 —— Configure the receive version of the interface to RIPv1.

2 —— Configure the receive version of the interface to RIPv2.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the receive version of VLAN 1 to RIPv1:

```
Device (config)#interface vlan 1
Device (config-if)#ip rip receive version 1
```

58.17 ip rip send version

Description

The **ip rip send version** command is used to configure the version of RIP packets sent by the interface. If the send version of an interface is not configured, it will be determined by the global configuration. To restore the default configuration, please use the **no ip rip receive version** command.

Syntax

ip rip send version { 1 | 2 }

no ip rip send version

Parameter

1 —— Configure the send version of the interface to RIPv1.

2 —— Configure the send version of the interface to RIPv2.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the send version of VLAN 1 to RIPv1:

```
Device (config)#interface vlan 1
Device (config-if)#ip rip send version 1
```

58.18 ip rip split-horizon

Description

The **ip rip split-horizon** command is used to configure the split horizon function of the interface. This function is enabled by default. When this function is enabled, RIP will not send routing entries learned from this interface out of this interface. When this function is disabled, RIP will only send routing entries according to the routing table. To disable this function, please use the **no ip rip split-horizon** command.

Syntax

ip rip split-horizon [poison-reverse]

no ip rip split-horizon

Parameter

poison-reverse —— Enable the poison-reverse function of the interface. After this function is enabled, the entries learned from the interface will have the metric set to 16 before being sent out. Disable the poison reversal function by configuring the ip rip split-horizon command.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the poison-reverse function of VLAN 1:

Device (config)#interface vlan 1

Device (config-if)#ip rip split-horizon poison-reverse

58.19 ip rip v2-broadcast

Description

The **ip rip v2-broadcast** command is used to enable the RIPv2 packet broadcast function of the interface. By default, RIPv2 messages are sent through multicast. After this function is enabled on an interface, RIPv2 messages on the interface are sent through broadcast. To disable this function, please use the **no ip rip v2-broadcast** command.

Syntax

ip rip v2-broadcast

no ip rip v2-broadcast

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the RIPv2 packet broadcast function of VLAN 1:

Device (config)#interface vlan 1

Device (config-if)#ip rip v2-broadcast

58.20 show ip rip

Description

The **show ip rip** command is used to display the RIP routing table.

Syntax

show ip rip [**vrf** *vrf-name*]

Parameter

vrf-name —— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIP routing table of VRF v1:

```
Device#show ip rip vrf v1
```

58.21 show ip rip status

Description

The **show ip rip status** command is used to display the RIP status.

Syntax

show ip rip [**vrf** *vrf-name*] **status**

Parameter

vrf-name —— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIP status of VRF v1:

```
Device#show ip rip status vrf v1
```

58.22 clear ip rip

Description

The **clear ip rip** command is used to clear the routing entries for RIP learning and re-request routing information from other devices.

Syntax

clear ip rip [**vrf** *vrf-name*]

Parameter

vrf-name —— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the routing entries for RIP learning and rerequest routing information from of VRF v1:

```
Device#clear ip rip vrf v1
```

Chapter 59 RIPng Configuration Commands

RIPng (RIP next generation) is a routing protocol that improves the RIP protocol in order to solve the compatibility problem between the RIP protocol and IPv6.

59.1 router ripng

Description

This **router ripng** command is used to enable the RIPng function. Only when the RIPng function is enabled can the global configuration of the RIPng function be performed. When the RIPng function is disabled, the global configuration of the RIPng function will be cleared. To disable this function, please use the **no router ripng** command. You can specify to create a RIPng instance under a certain VRF.

Syntax

router ripng [**vrf** *vrf-name*]

no router ripng [**vrf** *vrf-name*]

Parameter

vrf-name —— VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the RIPng function in VRF v1:

```
Device(config)#router ripng vrf v1
```

59.2 ipv6 rip enable

Description

The **ipv6 rip enable** command is used to enable the ripng function of the interface. This command only takes effect after the global Device of RIPng is enabled.To disable this function, please use **no ipv6 rip enable** command.

Syntax

ipv6 rip enable

no ipv6 rip enable

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the RIPng function of VLAN 1:

```
Device(config)#interface vlan 1
Device(config-if)# ipv6 rip enable
```

59.3 timer basic

Description

The **timer basic** command is used to configure the RIPng timer. To restore the timer configuration to its default, please use the **no timer basic** command.

Syntax

timer basic *update-value timeout-value garbage-collect-value*

no network

Parameter

update-value —— Routing table update time, ranging from 5 to 86400 seconds. The default value is 30.

timeout-value —— Routing table aging time, ranging from 5 to 86400 seconds. The default value is 180.

garbage-collect-value —— The expiration time after the routing entry is unreachable. When the entry is unreachable, the routing entry is removed

from the routing table after the expiration time. The range is 5~86400 seconds, and the default value is 120.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the routing table update time to 50 seconds, the routing table aging time to 100 seconds, and the routing entry expiration time to 100 seconds:

```
Device(config-router)#timer basic 50 100 100
```

59.4 default-metric

Description

The **default-metric** command is used to set the default metric for redirect routes. To restore the default configuration, please use the **no default-metric** command.

Syntax

default-metric *metric*

no default-metric

Parameter

metric —— The default metric of the redirect route, ranging from 1 to 15, and the default value is 1.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set the default metric for redirection routes to 5:

```
Device(config-router)#default-metric 5
```

59.5 redistribute

Description

The **redistribute** command is used to set RIPng to redirect external routes. Its no command has two forms: if it does not contain the metric parameter, it is used to disable the redirection function of the corresponding external route. If it contains the metric parameter, it is used to restore the metric used for redirect routes to the default value.

Syntax

redistribute { ospfv3 | static } [**metric** *metric-value*]

no redistribute { ospfv3 | static } [**metric**]

Parameter

ospfv3 —— Enable RIPng redirect OSPFv3 routing function.

static —— Enable RIPng redirect static routing function.

metric-value —— The metric of the redirect route.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Set RIPng to redirect OSPFv3, and set metric to 3:

```
Device(config-router)#redistribute ospfv3 metric 3
```

59.6 allow-ecmp

Description

The **allow-ecmp** command is used to enable the ECMP function. To disable this function, please use the **no allow-ecmp** command.

Syntax

allow-ecmp

no allow-ecmp

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the ECMP function of RIPng:

```
Device(config-router)#allow-ecmp
```

59.7 default-information originate

Description

The **default-information originate** command is used to introduce a default route into RIPng. To disable this function, please use the **no default-information originate** command.

Syntax

default-information originate

no default-information originate

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Introduce a default route into RIPng:

```
Device(config-router)#default-information originate
```

59.8 passive-interface

Description

The **passive-interface** command is used to configure the interface not to send RIPng packets but only to receive RIPng packets. A unicast response will be sent out when a neighbor is configured at the same time.To disable this function, please use the **no passive-interface** command.

Syntax

passive-interface interface { fastEthernet | gigabitEthernet | hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } *interface-value*

no passive-interface interface { fastEthernet | gigabitEthernet | hundred-gigabitEthernet | loopback | port-channel | ten-gigabitEthernet | twentyFive-gigabitEthernet | two-gigabitEthernet | vlan } *interface-value*

Parameter

interface-value —— Specify the interface to be configured as passive-interface.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure VLAN 2 as passive-interface:

```
Device(config-router)# passive-interface interface vlan 2
```

59.9 ip rip split-horizon

Description

The **ipv6 rip split-horizon** command is used to configure the split horizon function of the interface. This function is enabled by default. When this function is enabled, RIPng will not send routing entries learned from this interface out of this interface. When this function is disabled, RIPng will only send routing entries according to the routing table. To disable this function, please use the **no ipv6 rip split-horizon** command.

Syntax

ipv6 rip split-horizon [poison-reverse]

no ipv6 rip split-horizon

Parameter

poison-reverse: Enable the poison-reverse function of the interface. After this function is enabled, the entries learned from the interface will have the metric set to 16 before being sent out. Disable the poison reversal function by configuring the ipv6 rip split-horizon command.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Configure the poison-reverse function of VLAN 1:

```
Device (config)#interface vlan 1

Device (config-if)#ipv6 rip split-horizon poison-reverse
```

59.10 show ipv6 rip

Description

The **show ipv6 rip** command is used to display the RIPng routing table.

Syntax

show ipv6 rip [**vrf** *vrf-name*]

Parameter

vrf-name —— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIPng routing table in VRF v1:

```
Device#show ipv6 rip vrf v1
```

59.11 show ipv6 rip status

Description

The **show ipv6 rip status** command is used to display the RIPng status.

Syntax

show ipv6 rip [**vrf** *vrf-name*] **status**

Parameter

vrf-name —— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

View the RIPng status in VRF v1:

```
Device#show ipv6 rip status vrf v1
```

59.12 clear ipv6 rip

Description

The **clear ipv6 rip** command is used to clear the routing entries for RIPng learning and re-request routing information from other devices.

Syntax

clear ipv6 rip [**vrf** *vrf-name*]

Parameter

vrf-name —— VRF instance name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the routing entries for RIPng learning and rerequest routing information from other devices:

```
Device#clear ipv6 rip vrf v1
```

Chapter 60 OSPF Configuration Commands

OSPF is an Interior Gateway Protocol (IGP) designed expressly for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

Currently, OSPF Version 2 (RFC2328) is used for the IPv4 protocol; Use OSPF Version 3 (RFC2740) for IPv6 protocol. Unless otherwise specified, the OSPF referred to in this chapter is OSPF Version 2.

60.1 router ospf

Description

When the OSPFv2 instance specified by the process-id has not been created, this command is used to create an OSPFv2 instance and enter Router configuration mode. If a vrf name is specified when using the command, it indicates that this OSPFv2 instance belongs to the specified VRF instance. If the vrf parameter is not specified, the created OSPFv2 instance will belong to the public network. When the OSPFv2 instance specified by the process-id already exists, using this command with the correct vrf name (or without the vrf parameter) will allow entry into Router configuration mode. The no command is used to delete the OSPFv2 instance. When the vrf parameter is not specified, the corresponding instance will be deleted based on the process-id.

Syntax

router ospf *process-id* [**vrf** *vrf-name*]

no router ospf *process-id* [**vrf** *vrf-name*]

Parameter

process-id—— Process ID, ranging from 1 to 65535. Sixteen processes can be created at most.

vrf-name—— VRF instance name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Create an OSPFv2 instance with process ID 1 and add it to vrf1:

```
Device(config)#router ospf 1 vrf vrf1
```

60.2 router-id

Description

The **router-id** command is used to configure the router ID. To delete the configured router-id, please use the **no router-id** command.

Syntax

Router-id *router-id*

no router-id

Parameter

router-id—— The route ID in the format of dotted decimal notation. 0.0.0.0 is illegal.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the router ID of OSPF routing process 1 as 1.1.1.1:

```
Device(config)#router ospf 1
Device(config-router)#router-id 1.1.1.1
```

60.3 network

Description

This **network** command is used to configure the network of a specified area. All the interfaces fallen into the configured network will belong to this area. To delete the specified network and its corresponding interfaces from this area, please use the **no network** command.

Syntax

network *ip-address wildcard-mask* **area** *area-id*

no network *ip-address wildcard-mask* **area** *area-id*

Parameter

ip-address —— The IP address of the network.

wildcard-mask —— The wildcard mask of the network (such as 0.0.0.255). The subnet mask is also compatible (such as 255.0.0.0).

area-id —— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

Command Mode

Router Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the network 192.168.0.0/24 in the area 0.0.0.0:

```
Device(config)#router ospf 1
Device(config-router)# network 192.168.0.0 255.255.255.0 area 0.0.0.0
```

60.4 maximum-paths

Description

The **maximum-paths** command is used to configure the maximum number of the equal-cost multipath routings. To restore to default value, please use the **no maximum-paths** command.

Syntax

maximum-paths *number*

no maximum-paths

Parameter

number —— The maximum number of the equal-cost multipath routings, ranging from 1 to 32. The default value is 32.

Command Mode

Router Configuration Mode

Example

Configure the maximum number of the equal-cost multipath routings as 2:

```
Device(config)#router ospf 1

Device(config-router)#maximum-paths 2
```

60.5 redistribute

Description

The **redistribute** command is used to configure the ASBR to redistribute the external routes from other routing protocols to the OSPF domain in type-5 LSAs. To restore the certain optional parameters to default values, please use the **no redistribute** command with corresponding parameters.

Syntax

redistribute { **connected** | **static** /**rip** | **ospf** *process-id*} [**metric** *cost*] [**metric-type** *type*]

no redistribute { **connected** | **static** /**rip** | **ospf** *process-id*} [**metric** *cost*] [**metric-type** *type*]

Parameter

connected —— Specify the external route type as connected.

static —— Specify the external route type as static.

rip —— Specify the external route type as RIP.

ospf —— Specify the external route type as OSPF.

process-id —— The OSPF routing process ID, ranging from 1 to 65535. It's not allowed to redirect to the own process, for example, OSPF process 1 cannot redirect itself.

cost —— The cost of the external routes, ranging from 1 to 16777214. Its default value is defined in the command default-metric.

type —— The type of the external routes, either 1 or 2. The default value is 2.

Command Mode

Router Configuration Mode

Example

Redistribute the RIP routes from the external and advertise them as type 1 external routes in the OSPF domain:

```
Device(config)#router ospf 1
Device(config-router)#redistribute rip metric-type 1
```

60.6 default-metric

Description

The **default-metric** command is used to configure the default cost of the redistributing external route. To restore to the default value, please use the **no default-metric** command.

Syntax

default-metric *cost*

no default-metric

Parameter

cost—— The default cost of the redistributing external route, ranging form 1 to 16777214.

Command Mode

Router Configuration Mode

Example

Configure the default cost of the redistributing external route as 12:

```
Device(config)#router ospf 1
Device(config-router)#default-metric 12
```

60.7 default-metric

Description

The **default-information originate** command is used to advertise the default route as AS-External LSA. To cancel the advertisement of the default route, please use the **no default-information originate** command without any optional parameters. To restore the certain parameters to default values,

please use the **no default-information originate** command with corresponding parameters.

Syntax

default-information originate [**always**] [**metric** *cost*] [**metric-type** *type*]

no default-information originate [**always**] [**metric** *cost*] [**metric-type** *type*]

Parameter

always —— OSPF will advertise the default route whether there is default route is the IP routing table or not. If the parameter is not configured, OSPF will advertise the default route only when there is default route in the IP routing table.

cost —— The default cost of the default route, ranging form 1 to 16777214. Its default value is 1.

type —— The type of the external routes, either 1 or 2. The default value is 2.

Command Mode

Router Configuration Mode

Example

Configure OSPF to advertise the default route whether there is default route is the IP routing table or not:

```
Device(config)#router ospf 1
Device(config-router)#default-information originate always
```

60.8 auto-cost

Description

The **auto-cost** command is used to enable the auto computing function of the interface cost and configure the reference bandwidth. The interface cost is the ratio of the reference bandwidth to the interface bandwidth. To restore the reference bandwidth to default value, please use the **no auto-cost reference-bandwidth** command.

Syntax

auto-cost reference-bandwidth *bandwidth*

no auto-cost reference-bandwidth

Parameter

bandwidth —— The reference bandwidth, ranging from 1 to 4294967 Mbps. Its default value is 100Mbps.

Command Mode

Router Configuration Mode

Example

Enable the auto computing function of the interface cost and configure the reference bandwidth as 10000 Mbps:

```
Device(config)#router ospf 1
Device(config-router)#auto-cost reference-bandwidth 10000
```

60.9 distance

Description

The **distance** command is used to configure the OSPF administrative distance. To restore to the default distance, please use the **no distance** command. The administrative distance represents the priority of the routes. The smaller administrative distance corresponds to higher priority. When different routing protocols possess the same route to the same destination, the route with the highest priority will be selected to add to the IP routing table according to the administrative distance.

Syntax

distance *administrative-distance*

no distance

Parameter

administrative-distance —— Routing administrative distance, ranging from 1 to 255. Its default value is 110. When this value is set to 255, it indicates that the source of routing information is unreliable and all related routes are ignored.

Command Mode

Router Configuration Mode

Example

Configure the OSPF routing administrative distance as 100:

```
Device(config)#router ospf 1
Device(config-router)#distance 100
```

60.10 timers throttle spf

Description

The **timers throttle spf** command is used to configure the computing delay and interval of the SPF, thus preventing the consumption of the CPU and memory caused by frequent SPF computing. To restore to the default value, please use the **no timers throttle spf** command.

Syntax

timers throttle spf *spf-delay spf-holdtime spf-max-holdtime*

no timers throttle spf

Parameter

spf-delay —— The delay time of the SPF computing, ranging from 1 to 600000 milliseconds. The default value is 0 milliseconds.

spf-holdtime —— The minimum interval between two SPF computings, ranging from 1 to 600000 milliseconds. The default value is 50 milliseconds.

spf-max-holdtime —— The Maximum interval between two SPF computings, ranging from 1 to 600000 milliseconds. The default value is 5000 milliseconds.

Command Mode

Router Configuration Mode

Example

Configure the computing delay and interval of the SPF as 10 seconds:

```
Device(config)#router ospf 1
Device(config-router)#timers throttle spf 10000 10000 50000
```

60.11 compatible rfc 1583

Description

The **compatible rfc 1583** command is used to configure the OSPF's compatibility for the routing rules in the RFC 1583. To cancel the compatibility, please use the **no compatible rfc1583** command. It is compatible by default.

Syntax

compatible rfc1583

no compatible rfc1583

Command Mode

Router Configuration Mode

Example

Configure the OSPF's compatibility for the routing rules in RFC 1583:

```
Device(config)#router ospf 1
Device(config-router)#compatible rfc1583
```

60.12 area stub

Description

The **area stub** command is used to define an area as a stub area. To restore the stub area to a normal one, please use the **no area stub** command. To restore the certain parameters to default values, please use the **no area stub** command with corresponding parameters.

Syntax

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

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

Parameter

area-id —— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

no-summary —— Configure the stub are as a totally stub area, where the ABR advertises neither the destinations in other areas nor the external routes. The stub area is not a totally stub area by default

Command Mode

Router Configuration Mode

Example

Configure the area 1 as a totally stub area:

```
Device(config)#router ospf 1
Device(config-router)# area 1 stub no-summary
```

60.13 area nssa

Description

The **area nssa** command is used to define an area as a NSSA area. To restore the NSSA area to a normal one, please use the **no area nssa** command without any optional parameters. To restore the certain parameters to default values, please use the **no area nssa** command with corresponding parameters.

Syntax

area *area-id* **nssa [no summary | default-information-originate [metric** *cost* **] [metrictype** *type***]]**

no *area-id* **nssa [no summary | default-information-originate [metric** *cost* **] [metrictype** *type***]]**

Parameter

area-id —— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

no-summary —— Configure the NSSA area as a totally NSSA area, where the ABR advertises neither the destinations in other areas nor the external routes. The NSSA area is not a totally NSSA area by default.

default-information-originate —— Enable or disable advertising default route into NSSA area by sending a NSSA-External LSA. OSPF will not advertise default route if this parameter is not specified

cost —— The default cost of the default route, ranging form 1 to 16777214. Its default value is 1.

type —— The type of the external routes, either 1 or 2. The default value is 2.

Command Mode

Router Configuration Mode

Example

Configure the Area 1 as a totally NSSA area:

```
Device(config)#router ospf 1
Device(config-router)# area 1 nssa no-summary
```

60.14 area default-cost

Description

The **area default-cost** command is used to configure the cost of default route sent from ABR to stub or NSSA area.

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter

area-id —— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

cost —— The cost value. It ranges from 1 to 16777214 and the default value is 1.

Command Mode

Router Configuration Mode

Example

Configure the cost of default route sent to Area 1 as 10:

```
Device(config)#router ospf 1
Device(config-router)#area 1 nssa
Device(config-router)#area 1 default-cost 10
```

60.15 area range

Description

The **area range** command is used to configure a summary route. To delete this route, please use the **no area range** command. By default no route is summarized.

This command is only used with the ABR to summarize the route information of a certain area. The ABR only sends one summarized route of the routes in the aggregated segment to the other areas. An area can be configured with multiple summary segments, which can be aggregated by OSPF.

If the no area range command is configured, the formally summarized routes will be redistributed.

Syntax

area *area-id* **range** *ip-address mask* [**advertise**] [**cost** *cost*] [**not-advertise**]

no area *area-id* **range** *ip-address mask* [**advertise**] [**cost** *cost*] [**not-advertise**]

Parameter

area-id —— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

ip-address —— The destination of the aggregated route.

mask —— The network mask of the aggregated route, in the format of dotted decimal notation.

advertise —— Allow route aggregation of ABR broadcast.

not-advertise —— Suppress route aggregation of ABR broadcast.

cost —— The cost of the aggregated route, ranging from 1 to 16777214. The default value is the maximum one of all the aggregated routes. The cost parameter can be configured only when the advtise parameter is enabled. When configured as not-advtise, the cost parameter will be restored to the default value.

Command Mode

Router Configuration Mode

Example

Configure one aggregated route 100.100.0.0/16 with the cost 10 in the Area 0:

```
Device(config)#router ospf 1
Device(config-router)#area 0 range 100.100.0.0 255.255.0.0 cost 10
```

60.16 area authentication

Description

The **area authentication** command is used to configure the authentication type of the ospf process. The process is not authenticated by default. To restore to default value, please use the **no area authentication** command.

Syntax

area *area-id* **authentication** [message-digest]

no area authentication

Parameter

area-id —— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 0 to 4294967295.

message-digest —— Configure the configuration type as MD5.

If no authentication mode is specified here, the default mode will be simple authentication.

Command Mode

Router Configuration Mode

Example

Configure the authentication method to MD5 in the Area 0:

```
Device(config)#router ospf 1
Device(config-router)#area 0 authentication message-digest
```

60.17 area virtual-link

Description

The **area virtual-link** command is used to configure the virtual-link. To delete the configured virtual-link, please use the **no area virtual-link** without any optional parameters. To restore the certain parameters to default values, please use the **no area virtual-link** command with corresponding parameters.

Syntax

area *transit-area* **virtual-link** *router-id* [**dead-interval** *dead-interval*] [**hello-interval** *hello-interval*] [**retransmit-interval** *rtx-interval*] [**transmit-delay** *trans-delay*]

no area *transit-area* **virtual-link** *router-id*

Parameter

transit-area —— The area ID, in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id—— The ID of the neighboring router on the opposite end of the virtual link, in the format of dotted decimal notation.

hello-interval—— The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

dead-interval—— The time after which the neighbor becomes invalid. It ranges from 1 to 65535 seconds and the default value is 4 times as the hello-interval.

rtx-interval—— The retransmission interval of the LSA, DD and LSR packets. It ranges from 1 to 65535 seconds and the default value is 5 seconds.

trans-delay—— The LSA transmission delay. It ranges from 1 to 65535 seconds and the default value is 1 seconds.

Command Mode

Router Configuration Mode

Example

Configure a virtual-link with the transmission area as Area 1 and the ID of the neighboring router on the other endpoint as 1.1.1.1:

```
Device(config)#router ospf 1
Device(config-router)#area 1 virtual-link 1.1.1.1
```

60.18 area virtual-link authentication

Description

The **area virtual-link authentication** command is used to configure the authentication type of the virtual link. The virtual link is not authenticated by default. To restore to default value, please use the **no area virtual-link authentication** command.

Syntax

area *transit-area* **virtual-link** *router-id* **authentication** [message-digest | null]

no area *transit-area* **virtual-link** *router-id* **authentication**

Parameter

transit-area—— The transition area ID in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id—— The ID of the neighboring router on the other endpoint of the virtual link, in the format of dotted decimal notation.

message-digest —— Configure the configuration type as MD5.

null —— No authentication. By default it is no authentication.

If no authentication mode is specified here, the default mode will be simple authentication.

Command Mode

Router Configuration Mode

Example

Configure simple authentication as the authentication mode of a virtual-link with the transmission area as Area 2 and the ID of the neighboring router on the other endpoint as 3.3.3.3:

Device(config)#router ospf 1

Device(config-router)#area 2 **virtual-link** 3.3.3.3 **authentication**

60.19 area virtual-link authentication-key

Description

The **area virtual-link authentication-key** command is used to configure the simple authentication key. To delete the key, please use the **no area virtual-link authentication-key** command.

Syntax

area *transit-area* **virtual-link** *router-id* **authentication-key [0|7]***password*

no area *transit-area* **virtual-link** *router-id* **authentication-key**

Parameter

transit-area—— The transition area ID in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id—— The ID of the neighboring router on the other endpoint of the virtual link, in the format of dotted decimal notation.

[0|7] —— Key form, 0 represents plaintext, 7 represents ciphertext.

password—— A string from 1 to 8 alphanumeric characters or symbols. The password is case-sensitive, and cannot contain question marks. By default, it is empty.

Command Mode

Router Configuration Mode

Example

Configure the authentication mode of a virtual-link as simple authentication, with the transmission area as Area 2 and the ID of the neighboring router on the other endpoint as 3.3.3.3, and the authentication key as 123456:

Device(config)#router ospf 1

Device(config-router)#area 2 **virtual-link** 3.3.3.3 **authentication-key**

123456

60.20 area virtual-link message-digest-key

Description

The **area virtual-link message-digest-key** is used to configure the MD5 authentication ID and key of the virtual-link. To delete the specified configuration, please use the **no area virtual-link message-digest- key** command.

Syntax

area *transit-area* **virtual-link** *router-id* **message-digest-key** *id* **md5 [0|7]** *password*

no area *transit-area* **virtual-link** *router-id* **message-digest-key** *id*

Parameter

transit-area —— The transition area ID in the format of an IP address in dotted decimal notation or decimal value ranging from 1 to 4294967295.

router-id —— The ID of the neighboring router on the other endpoint of the virtual link, in the format of dotted decimal notation.

id —— The key ID of the MD5, ranging from 1 to 255.

[0|7] —— Key form, 0 represents plaintext, 7 represents ciphertext.

password —— A string from 1 to 16 alphanumeric characters or symbols. The password is case-sensitive, and cannot contain question marks. By default, it is empty.

Command Mode

Router Configuration Mode

Example

Configure the authentication mode of a virtual-link as md5 authentication, with the transmission area as Area 2 and the ID of the neighboring router on the other endpoint as 3.3.3.3, with the authentication ID as 2 and the authentication key as 123456:

```
Device(config)#router ospf 1
Device(config-router)#area 2 virtual-link 3.3.3.3 message-digest- key 2
md5 123456
```

60.21 capability opaque

Description

The **capability opaque** is used to enable the Opaque LSA feature. To disable this feature, please use the **no capability opaque** command.

Syntax

capability opaque

no capability opaque

Parameter

None

Command Mode

Router Configuration Mode

Example

Enable the Opaque LSA feature:

```
Device(config)#router ospf 1
Device(config-router)#capability opaque
```

60.22 graceful-restart

Description

The **graceful-restart** is used to enable the OSPF GR feature. Before performing a graceful restart, ensure that the GR Restarter is configured with this feature. To disable this feature, please use the **no graceful-restart** command.

Syntax

graceful-restart

no graceful-restart

Parameter

None

Command Mode

Router Configuration Mode

Example

Enable the OSPF GR feature:

```
Device(config)#router ospf 1
Device(config-router)#graceful-restart
```

60.23 graceful-restart grace-period

Description

The **graceful-restart grace-period** is used to configure the graceful restart period, that is, the maximum time required for the graceful restart process. If the actual restart time exceeds this value, the graceful restart will fail. To restore the default configuration, please use the **no graceful-restart grace-period** command.

Syntax

graceful-restart grace-period *period*

no graceful-restart grace-period *period*

Parameter

period —— Graceful restart period, ranging from 1 to 1800 seconds, and the default value is 120.

Command Mode

Router Configuration Mode

Example

Configure the graceful restart period to 180 seconds:

Device(config)#router ospf 1

Device(config-router)#graceful-restart grace-period *180*

60.24 graceful-restart helper

Description

The **graceful-restart helper** is used to enable the GR Helper feature to assist the GR Restarter in its graceful restart process. To restore the default configuration, please use the **no graceful-restart helper** command.

Syntax

graceful-restart helper *[rid]*

no graceful-restart helper *[rid]*

Parameter

rid —— GR Helper is supported for the neighboring GR Restarter whose router-id is rid. If rid is not specified, GR Helper is supported for all neighboring GR Restarters by default.

Command Mode

Router Configuration Mode

Example

Configure GR Helper to support graceful restart for all neighboring GR Restarters:

Device(config)#router ospf 1

Device(config-router)#graceful-restart helper

60.25 graceful-restart helper planned-only

Description

The **graceful-restart helper planned-only** is used to configure the GR Helper to only support planned-only restart function, which is disabled by default. To restore the default configuration, please use the **no graceful-restart helper planned-only** command.

Syntax

graceful-restart helper planned-only

no graceful-restart helper planned-only

Parameter

None.

Command Mode

Router Configuration Mode

Example

Enable the GR Helper to support planned-only restart function:

```
Device(config)#router ospf 1
Device(config-router)#graceful-restart helper planned-only
```

60.26 graceful-restart helper strict-lsa-checking

Description

The **graceful-restart helper strict-lsa-checking** is used to configure the GR Helper to strictly check LSA, which is disabled by default. When this function is configured, once the LSAs of the GR Restarter and the GR Helper do not match, the graceful restart will be failed. To restore the default configuration, please use the **no graceful-restart helper strict-lsa-checking** command.

Syntax

graceful-restart helper strict-lsa-checking

no graceful-restart helper strict-lsa-checking

Parameter

None.

Command Mode

Router Configuration Mode

Example

Configure the GR Helper to strictly check LSA:

```
Device(config)#router ospf 1
Device(config-router)#graceful-restart helper strict-lsa-checking
```

60.27 ip ospf cost

Description

The **ip ospf cost** is used to configure the interface cost. To restore to the default value, please use the **no ip ospf cost** command.

Syntax

ip ospf cost *cost*

no ip ospf cost

Parameter

cost —— The interface cost, ranging from 1 to 65535. The default value is calculated according to the bandwidth.

Command Mode

Interface Configuration Mode

Example

Configure the cost of interface VLAN 2 as 10:

```
Device(config)#interface vlan 2
Device(config-if)# ip ospf cost 10
```

60.28 ip ospf retransmit-interval

Description

The **ip ospf retransmit-interval** command is used to configure the interval to retransmit the LSA, DD and LSR packets on the specified interface. To restore to default value, please use the **no ip ospf retransmit-interval** command.

Syntax

ip ospf retransmit-interval *interval*

no ip ospf retransmit-interval

Parameter

interval—— The retransmit interval, ranging from 1 to 65535 seconds. The default value is 5 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the retransmission interval of interface VLAN 2 as 10 seconds:

```
Device(config)#interface vlan 2
Device(config-if)#ip ospf retransmit-interval 10
```

60.29 ip ospf transmit-delay

Description

The **ip ospf transmit-delay** is used to configure the transmission delay of LSA on the specified interface. To restore to default value, please use the **no ip ospf transmit-delay**.

Syntax

ip ospf transmit-delay *delay*

no ip ospf transmit-delay

Parameter

delay—— The LSA transmission delay, ranging from 1 to 65535 seconds. The default value is 1 second.

Command Mode

Interface Configuration Mode

Example

Configure the LSA transmission delay of interface VLAN 2 as 2 seconds.

```
Device(config)#interface vlan 2
Device(config-if)#ip ospf retransmit-delay 2
```

60.30 ip ospf priority

Description

The **ip ospf priority** is used to configure the priority of the specified interface. To restore to the default value, please use the **no ip ospf priority** command.

Syntax

ip ospf priority *pri*

no ip ospf priority

Parameter

pri—— The priority of the interface, ranging from 0 to 255 and the default value is 1. Interface with the priority 0 cannot be elected as DR or BDR.

Command Mode

Interface Configuration Mode

Example

Configure the priority of the interface VLAN 2 as 1:

```
Device(config)#interface vlan 2
Device(config-if)#ip ospf priority 1
```

60.31 ip ospf hello-interval

Description

The **ip ospf hello-interval** is used to configure the hello intervals on the specified interface. To restore to the default value, please use the **no ip ospf hello-interval** command.

Syntax

ip ospf hello-interval *interval*

no ip ospf hello-interval

Parameter

Interval—— The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the interval of the hello packets sent on interface VLAN 2 as 20 seconds:

Device(config)#interface vlan 2

Device(config-if)#ip ospf hello-interval 20

60.32 ip ospf dead-interval

Description

The **ip ospf dead-interval** command is used to set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down. To restore to default value, please use the **no ip ospf dead-interval** command.

Syntax

ip ospf dead-interval *interval*

no ip ospf dead-interval

Parameter

Interval—— The interval of the hello packets, ranging from 1 to 65535 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Example

Configure the neighbor's failure interval on interface VLAN 2 as 50 seconds:

Device(config)#interface vlan 2

Device(config-if)#ip ospf dead-interval 50

60.33 ip ospf authentication

Description

The **ip ospf authentication** command is used to configure the authentication mode of the specified interface. To restore to default value, please use the **no ip ospf authentication** command.

Syntax

ip ospf authentication [**message-digest**] [**null**]

no ip ospf authentication

Parameter

message-digest—— Specify the authentication type as MD5.

null —— No authentication. By default it is no authentication.

If no authentication mode is specified here, the default mode will be simple authentication.

Command Mode

Interface Configuration Mode

Example

Configure the authentication type of interface VLAN 2 as MD5:

```
Device(config)#interface vlan 2
Device(config-if)#ip ospf authentication message-digest
```

60.34 ip ospf authentication-key

Description

The **ip ospf authentication-key** command is used to configure the key of the simple authentication. To cancel this configuration, please use the **no ip ospf authentication-key** command.

Syntax

ip ospf authentication-key *password*

no ip ospf authentication-key

Parameter

password—— Super password, a string from 1 to 8 alphanumeric characters or symbols. The password is case sensitive, allows spaces but ignores leading spaces, and cannot contain question marks. By default, it is empty.

Command Mode

Interface Configuration Mode

Example

Configure the authentication mode of interface VLAN 2 as simple authentication, and the password as 123:

```
Device(config)#interface vlan 2

Device(config-if)#ip ospf authentication-key 123
```

60.35 ip ospf message-digest-key

Description

The **ip ospf message-digest-key** is used to configure the ID and password of the md5 authentication on the specified interface. To cancel the configuration, please use **no ip ospf message-digest-key** command.

Syntax

ip ospf message-digest-key *id* **md5** *password*

no ip ospf message-digest-key *id*

Parameter

id—— The ID of the md5 authentication key, ranging from 1 to 255.

password—— A string from 1 to 16 alphanumeric characters or symbols. The password is case sensitive, and cannot contain question marks. Key configuration is required to take effect.

Command Mode

Interface Configuration Mode

Example

Configure md5 authentication key ID as 1 and password as abc on interface VLAN 2:

```
Device(config)#interface vlan 2

Device(config-if)#ip ospf message-digest-key 1 md5 abc
```

60.36 ip ospf network

Description

The **ip ospf network** command is used to configure the network type on the specified interface. To restore to default, please use the **no ip ospf network** command.

Syntax

ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ip ospf network

Parameter

broadcast —— The broadcast network type. It is the default value.

non-broadcast —— The NBMA network type.

point-to-multipoint —— The point-to-multipoint network type.

point-to-point —— The point-to-point network type.

Command Mode

Interface Configuration Mode

Example

Configure the network type on interface VLAN 2 as broadcast:

```
Device(config)#interface vlan 2

Device(config-if)#ip ospf network broadcast
```

60.37 ip ospf mtu-ignore

Description

The **ip ospf mtu-ignore** command is used to ignore the MTU check in the DD exchanging process. This check is scheduled by default and the adjacency relationship will not establish if the MTUs are not matched. To restore to the default value, please use the **no ip ospf mtu-ignore** command.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Command Mode

Interface Configuration Mode

Example

Configure interface VLAN 2 to ignore the MTU field check in the DD exchange process:

```
Device(config)#interface vlan 2
Device(config-if)#ip ospf mtu-ignore
```

60.38 ip ospf passive

Description

The **ip ospf passive** command is used to prevent an interface from sending OSPF packets. To restore to the default settings, please use **no ip ospf passive** command. The interface is allowed to send OSPF packets by default.

Syntax

ip ospf passive

no ip ospf passive

Command Mode

Interface Configuration Mode

Example

Prevent interface VLAN 2 from sending OSPF packets:

```
Device(config)#interface vlan 2
Device(config-if)#ip ospf passive
```

60.39 clear ip ospf

Description

The **clear ip ospf** command is used to reset the OSPF process, which will clear all the dynamic information. The **clear ip ospf process** command will reset all the OSPF processes.

Syntax

clear ip ospf [*process-id*]

clear ip ospf process

Parameter

process-id—— The process ID, ranging from 1 to 65535.

Command Mode

Privileged EXEC Mode

Example

Reset all the OSPF processes:

```
Device#clear ip ospf process

Reset selected OSPF processes? (Y/N):y
```

60.40 show ip ospf

Description

The **show ip ospf** is used to display the global information of the OSPF process.

Syntax

show ip ospf [*process-id*]

Parameter

process-id—— The process ID, ranging from 1 to 65535. The global information of all the OSPF processes will be displayed if no process-id is specified.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the global information of all the OSPF processes:

```
Device#show ip ospf
```

60.41 show ip ospf database

Description

The **show ip ospf database** command is used to display the LSDB. The detailed LSA information will be displayed if the LSA type is specified. The LSDB summary information will be displayed if the LSA type is not specified.

Syntax

show ip ospf [*process-id*] **database** [asbr-summary | external | network | nssa-external | router | summary]

Parameter

process-id —— The process ID, ranging from 1 to 65535. The LSDBs of all processes will be displayed if no process ID is specified.

asbr-summary | external | network | nssa-external | router | summary —— The LSA type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the detailed information of router-LSA in process 1:

```
Device#show ip ospf 1 database router
```

60.42 show ip ospf interface

Description

The **show ip ospf interface** command is used to display the interface information.

Syntax

show ip ospf [*process-id*] **interface** [*interface-name interface-number*]

Parameter

process-id —— The process ID. The information of all the processes will be displayed if process ID is not specified.

interface-name interface-number —— Specify the interface name and number to display the interface's detailed information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the information of the interfaces in all the OSPF processes:

```
Device#show ip ospf interface
```

60.43 show ip ospf neighbor

Description

The **show ip ospf neighbor** command is used to display information of the OSPF neighbor.

Syntax

show ip ospf [*process-id*] **neighbor** [**detail |** *interface-name interface-number*]

Parameter

process-id —— The process ID, ranging from 1 to 65535. The neighbors' information of all processes will be displayed if no process ID is specified.

Detail —— The detailed information of the neighbor.

interface-name interface-number —— Specify the interface name and number to display the neighbor's detailed information on this interface.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the neighbors' detailed information in process 1:

```
Device#show ip ospf 1 neighbor detail
```

60.44 show ip ospf border-routers

Description

The **show ip ospf border-routers** is used to display the routing tables of the ABR/ASBR.

Syntax

show ip ospf [*process-id*] **border-routers**

Parameter

process-id—— The process ID, ranging from 1 to 65535. The ABR/ASBR routing tables of all processes will be displayed if no process ID is specified.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ABR/ASBR routing tables of all the OSPF processes:

```
Device#show ip ospf border-routers
```

60.45 show ip ospf route

Description

The **show ip ospf route** command is used to display the OSPF routing table.

Syntax

show ip ospf route

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the routing tables of OSPF:

```
Device#show ip ospf route
```

60.46 show ip ospf [process-id] graceful-restart helper

Description

The **show ip ospf [process-id] graceful-restart helper** command is used to view the status and configuration information of the GR Helper and the reason of last exit.

Syntax

show ip ospf *[process-id]* **graceful-restart helper**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the status and configuration information of the GR Helper and the reason of last exit:

```
Device# show ip ospf graceful-restart helper
```

Chapter 61 Service Port Profile Configuration Commands

Service port profiles are configured by the customer or network administrator to provide a means of applying common settings to multiple ONUs in a streamlined and efficient manner. These profiles define the parameter settings for services hosted on ONUs managed by the OLT.

It's important to note that there may not be a concept of a "default service port profile" in the sense that it is automatically applied to all ONUs. Instead, the network administrator typically needs to create and configure service port profiles as needed to meet specific service requirements. This includes defining parameters such as ONU port numbers, multicast settings, and port configurations for transmitting user services.

When the predefined or manually created service port profiles do not satisfy the current or future service demands, the customer or network administrator can add new profiles or modify existing ones to better align with their needs. This flexibility allows for the efficient management of large-scale deployments with varying service requirements.

61.1 ont-srvport-profile gpon

Description

The **ont-srvport-profile gpon** command is used to create a service port profile. To disable the service port profile, please use **no ont-srvport-profile gpon** command.

Syntax

ont-srvport-profile gpon {[profile-id *profile-id*] [profile-name *profile-name*]}

no ont-srvport-profile gpon {[profile-id *profile-id*] | [profile-name *profile-name*]}

Parameter

profile-id—— The profile ID of the service profile. The value range is 1-127, and each profile ID value is unique. If you leave the profile ID as blank, the system autamatically assigns the profile ID.

profile-name—— The profile name of the service profile. It is 1-32 characters long and the names of different profiles cannot be the same. If you leave the profile name as blank, the system autamatically assigns the profile name.

If both profile-id and profile-name are blank, the system will assign an idle ID and name. The no ont-srvport-profile command does not support both parameters being blank at the same time.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Add a service port profile named TP-Link:

```
Device(config)# ont-srvport-profile gpon profile-name TP-Link
```

61.2 show ont-srvport-profile gpon

Description

The **show ont-srvport-profile gpon** command is used to display the configuration information of the service port profile and the ONU binding status on the system.

Syntax

show ont-srvport-profile gpon {all | profile-id *profile-id* | profile-name *profile-name*}

Parameter

all —— Display all the service profiles.

profile-id —— The profile ID of the service profile. The profile ID is the unique identifier for the service profile.

profile-name —— The profile name of the service profile.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the service port profile of profile-id 1:

```
Device(config)# show ont-srvport-profile gpon profile-id 1
```

61.3 service-port

Description

The **service-port** command is used to configure the specific configuration of a service port entry in a service port profile.

Syntax

service-port service-port-index { adminstatus {enable | disable} | description *description* | inbound-traffic trafficProfileId | outbound-traffic trafficProfileId | statistics-performance {enable | disable} | config gem-id *gemId* svlan *svlanId* [user-vlan vlanId | user-pri vlanPri | ethertype {none | ipv4oe | ipv6oe | pppoe} | tag-action {default | transparent | translate | translate-add | add-double} | inner-vlan vlanId | inner-pri vlanPri | traffic-in trafficProfileId | traffic-out trafficProfileId | desc description | adminstatus {enable | disable} | statistic-performance {enable | disable}] }

Parameter

service-port-index—— Index ID of the service port configuration in the service port profile, ranging from 1 to 127

gemId—— Value of gemId, ranging from 1 to 1023

svlanId—— Value of svlanId, ranging from 1 to 4093

vlanId—— Value of vlanId, ranging from 1 to 4093

vlanPri—— Value of vlanPri, ranging from 0 to 7

trafficProfileId—— Traffic profile id in the system

Command Mode

ONT Service Port Profile Configuration Mode

Privilege Requirement

Only Admin and Operator level users have access to these commands.

Example

Enable the adminstatus of service port profile 1:

Device(config)# ont-srvport-profile gpon profile-id 1

Device(config-ont-srvportprofile)# service-port 1 adminstatus enable

61.4 show ont-srvport-profile gpon bound-info

Description

The **show ont-srvport-profile gpon bound-info** command is used to display the bound information of the service port profile.

Syntax

show ont-srvport-profile gpon bound info {all | profile-id *profile-id* | profile-name *profile-name*}

Parameter

all —— Display all the service profiles.

profile-id —— The profile ID of the service profile. The profile ID is the unique identifier for the service profile.

profile-name —— The profile name of the service profile.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the service port profile bound information of profile-id 1:

Device(config)# show ont-srvport-profile gpon bound info profile-id 1

Chapter 62 IPv4 IMPB Commands

You can bind the IP address, MAC address, VLAN and the connected Port number of the Host together, which can be the condition for the ARP Inspection and IP verify source to filter the packets.

62.1 ip source binding

Description

The **ip source binding** command is used to bind the IP address, MAC address, VLAN ID and the Port number together manually. You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN. To delete the IP-MAC–VID-PORT entry from the binding table, please use **no ip source binding index** command.

Syntax

ip source binding *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface** { **fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id*} { none | arp-detection | ip-verify-source | both }

no ip source binding index *ip-addr*

Parameter

hostname —— The Host Name, which contains 20 characters at most.

ip-addr —— The IP address of the Host.

mac-addr —— The MAC address of the Host.

vlan-id —— The VLAN ID needed to be bound, ranging from 1 to 4094.

port —— The number of port connected to the Host.

none | arp-detection | ip-verify-source | both ——The protect type for the entry. "arp-detection" indicates ARP detection; "ip-verify-source" indicates IP source filter; "none" indicates applying none; "both" indicates applying both.

ip-addr —— The IP address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Bind an ACL entry with the IP 192.168.0.1, MAC 00:00:00:00:00:01, VLAN ID 2 and the Port number 5 manually. And then enable the entry for the ARP detection:

Device(config)#ip source binding host1 192.168.0.1 00:00:00:00:00:01 **vlan** 2 **interface gigabitEthernet** 1/0/5 arp-detection

Delete the IP-MAC–VID-PORT entry with the index 5:

Device(config)#no ip source binding index 5

62.2 no ip source binding interface

Description

The **ip source binding interface** command is used to delete IMPB entries bound to a specified port in batches.

Syntax

no ip source binding interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

Parameter

port—— The number of port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete IMPB entries bound to port 1/0/1:

Device(config)# no ip source binding interface gigabitEthernet 1/0/1

62.3 ip dhcp snooping

Description

The **ip dhcp snooping** command is used to enable DHCP Snooping function globally. To disable DHCP Snooping function globally, please use **no ip dhcp snooping** command. DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ip dhcp snooping

no ip dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Snooping function globally:

```
Device(config)#ip dhcp snooping
```

62.4 ip dhcp snooping vlan

Description

The **ip dhcp snooping vlan** command is used to enable DHCP Snooping function on a specified VLAN. To disable DHCP Snooping function on this VLAN, please use **no ip dhcp snooping vlan** command.

Syntax

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the DHCP snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCP Snooping function on VLAN 1,4,6-7:

Device(config)#ip dhcp snooping vlan 1,4,6-7

62.5 ip dhcp snooping max-entries

Description

The **ip dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCP Snooping. To restore to the default setting, please use **no ip dhcp snooping max-entries** command.

Syntax

ip dhcp snooping max-entries *value*

no ip dhcp snooping max-entries

Syntax

value —— Enter the value of maximum number of entries that can be learned on the port via DHCP Snooping.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of entries that can be learned on port 1 as 100:

Device(config)#interface gigabitEthernet 1/0/1

Device(config-if)#ip dhcp snooping max-entries 100

62.6 ip dhcp snooping trust

Description

The **ip dhcp snooping trust** command is used to configure the trust status of a specified interface, and only DHCP Server connected to a trusted port can assign packets to clients. To delete the status, please use **no ip dhcp snooping trust** command.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable DHCP Snooping trust function for port 1/0/3:

Device(config)#interface gigabitEthernet 1/0/3

Device(config-if)#ip dhcp snooping trust

62.7 show ip source binding

Description

The **show ip source binding** command is used to display the IP-MAC-VID-PORT binding table.

Syntax

show ip source binding

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP-MAC-VID-PORT binding table:

```
Device(config)#show ip source binding
```

62.8 show ip dhcp snooping

Description

The **show ip dhcp snooping** command is used to display the running status of DHCP Snooping.

Syntax

show ip dhcp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of DHCP Snooping:

```
Device#show ip dhcp snooping
```

62.9 show ip dhcp snooping interface

Description

The **show ip dhcp snooping interface** command is used to display the DHCP Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

show ip dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Snooping configuration of all Ethernet ports and port channels:

Device#show ip dhcp snooping interface

Display the DHCP Snooping configuration of Gigabit Ethernet port 1/0/5:

Device#show ip dhcp snooping interface gigabitEthernet 1/0/5

Chapter 63 IPv6 IMPB Commands

You can bind the IPv6 address, MAC address, VLAN and the connected Port number of the Host together, which can be the condition for the ARP Inspection and IP verify source to filter the packets.

63.1 ipv6 source binding

Description

The **ipv6 source binding** command is used to bind the IPv6 address, MAC address, VLAN ID and the Port number together manually. You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN. To delete the IPv6-MAC–VID-PORT entry from the binding table, please use **no ipv6 source binding index** command.

Syntax

ipv6 source binding *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface** { **fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id*} { none | nd-detection | ipv6-verify-source | both }

no ipv6 source binding index *ipv6-addr*

Parameter

hostname ——The Host Name, which contains 20 characters at most.

Ipv6-addr —— The IP address of the Host.

mac-addr —— The MAC address of the Host.

vlan-id ——The VLAN ID needed to be bound, ranging from 1 to 4094.

port —— The number of port connected to the Host.

none | nd-detection | ipv6-verify-source | both ——The protect type for the entry. "nd-detection" indicates ND detection; "ipv6-verify-source" indicates IPv6 source filter; "none" indicates applying none; "both" indicates applying both.

Ipv6-addr —— The IPv6 address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

The following example shows how to bind an entry with the hostname host1, IPv6 address 2001:0:9d38:90d5::34, MAC address AA-BB-CC-DD-EE-FF, VLAN ID 10, port number 1/0/5, and enable this entry for ND Detection.

Device(config)# ipv6 source binding host1 2001:0:9d38:90d5::34 aa:bb:cc:dd:ee:ff **vlan** 10 **interface gigabitEthernet** 1/0/5 nd-detection

63.2 no ipv6 source binding interface

Description

The **ipv6 source binding interface** command is used to delete IMPB entries bound to a specified port in batches.

Syntax

no ipv6 source binding interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

Parameter

port—— The number of port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete IMPB entries bound to port 1/0/1:

Device(config)# no ipv6 source binding interface gigabitEthernet 1/0/1

63.3 ipv6 dhcp snooping

Description

The **ipv6 dhcp snooping** command is used to enable DHCPv6 Snooping function globally. To disable DHCPv6 Snooping function globally, please use **no ipv6 dhcp snooping** command. DHCPv6 Snooping functions to monitor the process of the Host obtaining the IP address from DHCPv6 server, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ipv6 dhcp snooping

no ipv6 dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Snooping function globally:

```
Device(config)#ipv6 dhcp snooping
```

63.4 ipv6 dhcp snooping vlan

Description

The **ipv6 dhcp snooping vlan** command is used to enable DHCP Snooping function on a specified VLAN. To disable DHCP Snooping function on this VLAN, please use **no ipv6 dhcp snooping vlan** command.

Syntax

ipv6 dhcp snooping vlan *vlan-range*

no ipv6 dhcp snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the DHCP snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DHCPv6 Snooping function on VLAN 1,4,6-7:

Device(config)#ipv6 dhcp snooping vlan 1,4,6-7

63.5 ipv6 dhcp snooping max-entries

Description

The **ipv6 dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCPv6 Snooping. To restore to the default setting, please use **no ipv6 dhcp snooping max-entries** command.

Syntax

Ipv6 dhcp snooping max-entries *value*

no ipv6 dhcp snooping max-entries

Syntax

value —— Enter the value of maximum number of entries that can be learned on the port via DHCPv6 Snooping.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of entries that can be learned on port 1 as 100:

Device(config)#interface gigabitEthernet 1/0/1

Device(config-if)#ipv6 dhcp snooping max-entries 100

63.6 ipv6 nd snooping

Description

The **ipv6 nd snooping** command is used to enable ND snooping function globally. To disable ND Snooping function globally, please use **no ipv6 nd snooping** command. ND Snooping functions to monitor the process of the duplication address detection, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ipv6 nd snooping

no ipv6 nd snooping

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ND snooping function globally:

Device(config)#ipv6 nd snooping

63.7 ipv6 nd snooping vlan

Description

The **ipv6 nd snooping vlan** command is used to enable ND snooping function on a specified VLAN. To disable ND Snooping function on this VLAN, please use **no ipv6 nd snooping vlan** command.

Syntax

ipv6 nd snooping vlan *vlan-range*

no ipv6 nd snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the ND snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ND snooping function on VLAN 1,4,6-7:

Device(config)#ipv6 nd snooping vlan 1,4,6-7

63.8 ipv6 nd snooping max-entries

Description

The **ipv6 nd snooping max-entries** command is used to specify the maximum number of binding entries that are allow to be bound to a port. To return the default, please use **no ipv6 nd snooping max-entries** command.

Syntax

ipv6 nd snooping max-entries *value*

no ipv6 nd snooping max-entries

Parameter

value —— Specify the maximum number of ND snooping entries on this interface.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of binding entries from ND Snooping of Gigabit Ethernet port 1/0/2 is 100:

```
Device(config)#interface gigabitEthernet 1/0/2
Device(config-if)#ipv6 nd snooping max-entries 100
```

63.9 show ipv6 source binding

Description

The **show ipv6 source binding** command is used to display the IPv6-MAC-VID- PORT binding table.

Syntax

show ipv6 source binding

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6-MAC-VID-PORT binding table:

```
Device(config)#show ipv6 source binding
```

63.10 show ipv6 dhcp snooping

Description

The **show ipv6 dhcp snooping** command is used to display the running status of DHCPv6 Snooping.

Syntax

show ipv6 dhcp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of DHCPv6 Snooping:

Device#show ipv6 dhcp snooping

63.11 show ipv6 dhcp snooping interface

Description

The **show ipv6 dhcp snooping interface** command is used to display the DHCPv6 Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

show ipv6 dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Snooping configuration of all Ethernet ports and port channels:

Device#show ipv6 dhcp snooping interface

Display the DHCPv6 Snooping configuration of Gigabit Ethernet port 1/0/5:

Device#show ipv6 dhcp snooping interface gigabitEthernet 1/0/5

63.12 show ipv6 nd snooping

Description

The **show ipv6 nd snooping** command is used to display the running status of ND Snooping.

Syntax

show ipv6 nd snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of ND Snooping:

```
Device#show ipv6 nd snooping
```

63.13 show ipv6 nd snooping interface

Description

The **show ipv6 nd snooping interface** command is used to display the ND Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

show ipv6 nd snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ND Snooping configuration of all Ethernet ports and port channels:

Device#show ipv6 nd snooping interface

Display the ND Snooping configuration of Gigabit Ethernet port 1/0/5:

Device#show ipv6 nd snooping interface gigabitEthernet 1/0/5

Chapter 64 DoS Defend Commands

DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host. With the DoS Defend enabled, the switch can analyze the specific field of the received packets and provide the defend measures to ensure the normal working of the local network.

64.1 ip dos-prevent

Description

The **ip dos-prevent** command is used to enable the DoS defend function globally. To disable the DoS defend function, please use **no ip dos-prevent** command.

Syntax

ip dos-prevent

no ip dos-prevent

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DoS defend function globally:

```
Device(config)#ip dos-prevent
```

64.2 ip dos-prevent type

Description

The **ip dos-prevent type** command is used to select the DoS Defend Type. To disable the corresponding Defend Type, please use **no ip dos-prevent type** command.

Syntax

ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf }

no ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf }

Parameter

land ——The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both of the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection.

scan-synfin ——The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal.

xma-scan ——The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.

null-scan ——The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.

port-less-1024 ——The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024.

blat ——The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker.

ping-flood ——The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for the system to respond to legal communication.

syn-flood ——The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.

win-nuke ——Because the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this

type of packets to the TCP port139 (NetBIOS) of the host with the Operation System bugs, which will cause the host with a blue screen.

ping-of-death ——Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer.

Note: ping-of-death is only available on certain devices.

smurf ——Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

Note: smurf is only available on certain devices.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the DoS Defend Type named Land attack:

```
Device(config)#ip dos-prevent type land
```

64.3 show ip dos-prevent

Description

The **show ip dos-prevent** command is used to display the DoS information of the detected DoS attack, including enable/disable status, the DoS Defend Type, the count of the attack, etc.

Syntax

show ip dos-prevent

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DoS information of the detected DoS attack globally:

```
Device(config)#show ip dos-prevent
```

Chapter 65 ARP Inspection Commands

ARP (Address Resolution Protocol) Detect function is to protect the switch from the ARP cheating, such as the Network Gateway Spoofing and Man-In-The-Middle Attack, etc.

65.1 ip arp inspection

Description

The **ip arp inspection** command is used to enable the ARP Detection function globally. To disable the ARP Detection function, please use **no ip arp detection** command.

Syntax

ip arp inspection

no ip arp inspection

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ARP Detection function globally:

```
Device(config)#ip arp inspection
```

65.2 ip arp inspection validate

Description

The **ip arp inspection validate** command is used to enable the switch to check whether the reveided ARP packet is illegal. To disable,the feature please use **no ip arp detection validate** command.

Syntax

ip arp inspection validate { src-mac | dst-mac | ip **}**

no ip arp inspection validate { src-mac | dst-mac | ip **}**

Parameter

src-mac —— Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.

dst-mac —— Enable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

ip —— Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet

```
Device(config)#ip arp inspection validate src-mac
```

65.3 ip arp inspection vlan

Description

The **ip arp inspection vlan** command is used to enable the ARP Detection function on VLANs. To disable the ARP Detection function on VLANs, please use **no ip arp detection vlan** command.

Syntax

ip arp inspection vlan *vlan-list*

no ip arp inspection vlan *vlan-list*

Parameter

vlan-list —— Enter the VLAN ID. The format is 1,5-9.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the ARP Detection function on VLAN 2:

```
Device(config)#ip arp inspection vlan 2
```

65.4 ip arp inspection vlan logging

Description

The **ip arp inspection vlan logging** command is used to enable the Log function on the specific VLAN. To disable the Log function on the VLAN, please use **no ip arp detection vlan logging** command.

Syntax

ip arp inspection vlan *vlan-list* **logging**

no ip arp inspection vlan *vlan-list* **logging**

Parameter

vlan-list —— Enter the VLAN ID. The format is 1,5-9.

logging —— Enable the Log feature to make the switch generate a log when an ARP packet is discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the log feature on VLAN 2:

```
Device(config)#ip arp inspection vlan 2 logging
```

65.5 ip arp inspection trust

Description

The **ip arp inspection trust** command is used to configure the port for which the ARP Detect function is unnecessary as the Trusted Port. To clear the Trusted Port list, please use **no ip arp detection trust** command .The specific ports, such as up-linked port and routing port and LAG port, should be set as Trusted Port. To ensure the normal communication of the switch, please configure the ARP Trusted Port before enabling the ARP Detect function.

Syntax

ip arp inspection trust

no ip arp inspection trust

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Gigabit Ethernet ports 1/0/2-5 as the Trusted Port:

Device(config)#interface range gigabitEthernet 1/0/2-5

Device(config-if-range)#ip arp inspection trust

65.6 ip arp inspection limit-rate

Description

The **ip arp inspection limit-rate** command is used to configure the ARP speed of a specified port. To restore to the default speed, please use **no ip arp inspection limit-rate** command.

Syntax

ip arp inspection limit-rate *value*

no ip arp inspection limit-rate

Parameter

value——The value to specify the maximum amount of the received ARP packets per second, ranging from 1 to 300 in pps(packet/second). By default, the value is 100.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum amount of the received ARP packets per second as 50 pps for Gigabit Ethernet port 5:

Device(config)#interface gigabitEthernet 1/0/5

Device(config-if)#ip arp inspection limit-rate 50

65.7 ip arp inspection burst-interval

Description

The **ip arp inspection burst-interval** command is used to configure the burst interval of a specified port. To restore to the default speed, please use **no ip arp inspection burst-interval** command.

Syntax

ip arp inspection burst-interval *value*

no ip arp inspection burst-interval

Parameter

value—— Specify a time range. If the speed of received ARP packets in this time range reaches the limit for this time range, the port will be shut down. The valid values are from 1 to 15 seconds, and the default value is 1 second.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the burst interval as 2 seconds for Gigabit Ethernet port 5:

Device(config)#interface gigabitEthernet 1/0/5

Device(config-if)#ip arp inspection burst-interval 2

65.8 ip arp inspection recover

Description

The **ip arp inspection recover** command is used to restore a port to the ARP transmit status from the ARP filter status.

Syntax

ip arp inspection recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Restore Gigabit Ethernet port 1/0/5 to the ARP transmit status:

Device(config)#interface gigabitEthernet 1/0/5

Device(config-if)#ip arp inspection recover

65.9 ip arp inspection exceed

Description

The **ip arp inspection exceed** command is used to configure the overspeed action. To delete this action, please use **no ip arp inspection exceed** command.

Syntax

ip arp inspection exceed [**drop | shutdown**] *recover-time*

no ip arp inspection exceed

Parameter

drop —— Drop messages when speeding.

shutdown —— Shut ports down when speeding.

recover-time —— Configure self-recovery time.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the overspeed action as dropping messages when speeding and self-recovery time as 2 seconds for Gigabit Ethernet port 5:

Device(config)#interface gigabitEthernet 1/0/5

Device(config-if)#ip arp inspection exceed drop 2

65.10 show ip arp inspection

Description

The **show ip arp inspection** command is used to display the ARP detection global configuration including the enable/disable status and the Trusted Port list.

Syntax

show ip arp inspection

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP detection configuration globally:

```
Device(config)#show ip arp inspection
```

65.11 show ip arp inspection interface

Description

The **show ip arp inspection interface** command is used to display the interface configuration of ARP detection.

Syntax

show ip arp inspection interface [**gigabitEthernet** *port*]

Parameter

port——The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Gigabit Ethernet port 1/0/1:

```
Device(config)#show ip arp inspection interface gigabitEthernet 1/0/1
```

Display the configuration of all Ethernet ports:

```
Device(config)#show ip arp inspection interface
```

65.12 show ip arp inspection vlan

Description

The **show ip arp inspection vlan** command is used to display the VLAN configuration of ARP detection.

Syntax

show ip arp inspection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP Inspection configuration of VLAN:

```
Device(config)#show ip arp inspection vlan
```

65.13 show ip arp inspection statistics

Description

The **show ip arp inspection statistics** command is used to display the number of the illegal ARP packets received.

Syntax

show ip arp inspection statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the number of the illegal ARP packets received:

```
Device(config)#show ip arp inspection statistics
```

65.14 clear ip arp inspection statistics

Description

The **clear ip arp inspection statistics** command is used to clear the statistic of the illegal ARP packets received.

Syntax

clear ip arp inspection statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Clear the statistic of the illegal ARP packets received:

```
Device(config)#clear ip arp inspection statistics
```

Chapter 66 ARP Scan Commands

ARP Scan actively probes a network range to discover IP-MAC pairs, generating candidate entries for IMPB (IP-MAC-Port Binding) configuration.

66.1 ip arp scan

Description

The **ip arp scan** command is used to scan a VLAN/IP range via ARP to discover devices and generate candidate IMPB entries.

Syntax

ip arp scan vlan *{vid}* **from** *{start-ip}* **to** *{end-ip}*

Parameter

vid —— Specify the VLAN ID to scan. It ranges from 1 to 4093.

start ip —— Specify the start IP address of the scan range.

end ip —— Specify the ending IP address of the scan range. The value must be greater than or equal to the start-ip, and the total range must not exceed 512 IP addresses. If the start-ip and end-ip are identical, only that single IP address is scanned.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Specify an ip arp scan:

```
Device(config)#ip arp scan vlan 1 from 192.168.0.1 to 192.168.1.255
```

66.2 ip arp scan apply

Description

The **ip arp scan apply** command is used to apply a candidate ARP scan entry to the active IMPB table.

Syntax

ip arp scan apply *{ip-address} {hostname} {acl-type}*

Parameter

ip-address ——Specify the IP address for the IMPB entry. It must be an IPv4 address present in the ARP scan results.

hostname ——Specify the hostname for the IMPB entry. Maximum length is 20 characters. Allowed characters are: letters (A-Z, a-z), digits (0-9), and the symbols: -_@:/.+#

acl-type ——Specify the protection type for the IMPB entry, which corresponds directly to the standard IMPB entry types:

none —— No associated protection.

arp-detection —— Used for ARP protection only.

ip-verify-source —— Used for IP source guard protection only.

both —— Used for both ARP and IP source guard protection.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Add the discovered IP and device details to the active IMPB entries.:

```
Device(config)#ip arp scan apply 192.168.0.128 host1 both
```

66.3 show ip arp scan

Description

The **show ip arp scan** command is used to display the last ARP scan results.

Syntax

show ip arp scan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the last ARP scan results.:

```
Device# show ip arp scan
```

Chapter 67 SDM Template Commands

This chapter describes how to configure the Switch Database Management (SDM) templates to allocate hardware resources on the switch for different uses.

67.1 sdm prefer

Description

The **sdm prefer** command is used to specify the SDM template to be used. The SDM template is used to allocate system resources to best support the features being used in your application. To return to use the default template, please use the **sdm prefer default** command. The template change will take effect after a reboot.

Syntax

sdm prefer { default | enterpriseV4 | enterpriseV6 | extacl | enterpriseMix | pca-default }

Parameter

default —— Specify the SDM template used in the switch as “default”.

enterpriseV4 —— Specify the SDM template used in the switch as “enterpriseV4”.

enterpriseV6 —— Specify the SDM template used in the switch as “enterpriseV6”.

extacl —— Specify the SDM template used in the switch as “extacl”, which provides more ACL support.

enterpriseMix —— Specify the SDM template used in the switch as “enterpriseMix”, which provides both IPv4/IPv6-ACL support and IMPBv4/v6 support.

pca-default —— Specify the SDM template used in the switch as “pca-default”, which provides packet-content-ACL support.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

Some models may not support **pca-default** template. Changes to the SDM preferences cannot take effect until reboot the switch.

Example

Specify the SDM template as enterpriseV4:

Device(config)# sdm prefer enterpriseV4

67.2 show sdm prefer

Description

The **show sdm prefer** command is used to display resource allocation of the current SDM template in use, or the SDM templates that can be used.

Syntax

show sdm prefer { used | default | enterpriseV4 | enterpriseV6 | extacl | enterpriseMix | pca-default}

Parameter

used —— Display the resource allocation of the template currently in use, and the template that will become active after a reboot.

default —— Display the resource allocation of the default template.

enterpriseV4 —— Display the resource allocation of the enterpriseV4 template.

enterpriseV6 —— Display the resource allocation of the enterpriseV6 template.

extacl —— Display the resource allocation of the extacl template.

enterpriseMix —— Specify the SDM template used in the switch as "enterpriseMix", which provides both IPv4/IPv6-ACL support and IMPBv4/v6 support.

pca-default —— Specify the SDM template used in the switch as "pca-default", which provides packet-content-ACL support.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the resource allocation of the template currently in use, and the template that will become active after a reboot:

```
Device(config)#show sdm prefer used
```

Chapter 68 IPv6 Neighbor Commands

IPv6 Neighbor Commands manage the mapping between IPv6 addresses and link-layer (MAC) addresses, serving the same core function as ARP does in IPv4. They are used on routers and switches to configure, monitor, and clear the Neighbor Discovery (ND) cache.

68.1 show ipv6 neighbors

Description

The **show ipv6 neighbors** command is used to query neighbor entries. It is used to view the mapping relationship between IPv6 addresses and MAC addresses or to obtain neighbor information for troubleshooting and diagnosis.

Syntax

show ipv6 neighbors

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Display the neighbor entries:

```
Device# show ipv6 neighbors
```

68.2 clear ipv6 neighbors

Description

The **clear ipv6 neighbors** command is used to clear neighbor entries. It is used to remove the mapping relationship between IPv6 addresses and MAC addresses.

Syntax

clear ipv6 neighbors

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Clear the neighbor entries :

```
Device# clear ipv6 neighbors
```

Chapter 69 File System Configuration Commands

File System Commands can be used to configure the File System.

69.1 copy

Description

The **copy** command is used to copy the specified file.

Syntax

copy {flash|usbflash1|usbflash2} {filename} {destination}

Parameter

flash|usbflash1|usbflash2 —— The flash type of the source file.

filename —— File name.

destination —— Copied file path.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Copy the specified file:

```
Device#copy flash test.txt usbflash1
```

69.2 cd

Description

The **cd** command is used to change the current file path.

Syntax

cd {filename|flash|usbflash1|usbflash2} [filename]

Parameter

filename|flash|usbflash1|usbflash2 —— The path that needs to be switched. If you enter filename, the file will be found in the current path by default.

filename —— Specify the file in the corresponding flash.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Change the current file path:

```
Device# cd usbflash1 test
```

69.3 dir

Description

The **dir** command is used to list files and subdirectories contained in the specified working directory.

Syntax

dir [flash|usbflash1|usbflash2] [filename]

Parameter

flash|usbflash1|usbflash2 —— Specify path.

filename —— Specify the file in the corresponding flash.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

List files and subdirectories contained in the specified working directory:

```
Device#dir flash
```

69.4 pwd

Description

The **pwd** command is used to display the absolute path name of the current working directory.

Syntax

pwd

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Display the absolute path name of the current working directory:

```
Device#pwd
```

69.5 rename

Description

The **rename** command is used to rename a file.

Syntax

rename {srcFilename} {dstFilename}

Parameter

srcFilename —— Source file name.

dstFilename —— Renamed file name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Rename a file:

```
Device#rename test1 test2
```

69.6 delete

Description

The **delete** command is used to delete a file.

Syntax

delete {filename|flash|usbflash1|usbflash2} [filename]

Parameter

filename|flash|usbflash1|usbflash2 —— The file that needs to be deleted. If you enter filename, the file will be found in the current working path by default.

filename —— Specify the file in the corresponding flash.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Delete a file:

```
Device# delete text.txt
```

69.7 ftp

Description

The **ftp** command is used to enter the FTP (File Transfer Protocol) view.

Syntax

ftp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enter the FTP view:

```
Switch#ftp
```

69.8 open

Description

The **open** command is used to connect to FTP server.

Syntax

open [ipv6] {hostIp}

Parameter

ipv6—— Specify the FTP server type as IPv6.

hostIp —— FTP server IP.

Command Mode

FTP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Connect to FTP server:

```
Device(ftp)#open 192.168.0.146
```

69.9 put

Description

The **put** command is used to upload files to FTP server.

Syntax

put {srcFilename} {dstFilename}

Parameter

srcFilename —— Source file name.

dstFilename —— Destination file name.

Command Mode

FTP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Upload files to FTP server:

```
Device(ftp)#put src.c dst.c
```

69.10 get

Description

The **get** command is used to download files from FTP server.

Syntax

get {srcFilename} {dstFilename}

Parameter

srcFilename —— Source file name.

dstFilename —— Destination file name.

Command Mode

FTP Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Download files from FTP server:

```
Switch(ftp)#get src.c dst.c
```

69.11 close

Description

The **close** command is used to close current FTP connection.

Syntax

close

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Close current FTP connection:

```
Device#close
```

Chapter 70 AAA Commands

AAA stands for authentication, authorization and accounting. This feature is used to authenticate users trying to log in to the switch or trying to access the administrative level privilege.

- **Applicable Access Application**

The authentication can be applied on the following access applications: Telnet, SSH and HTTP.

- **Authentication Method List**

A method list describes the authentication methods and their sequence to authenticate a user. The switch supports Login List for users to gain access to the switch, and Enable List for normal users to gain administrative privileges.

- **RADIUS/TACACS+ Server**

User can configure the RADIUS/TACACS+ servers for the connection between the switch and the server.

- **Server Group**

User can define the authentication server group with up to several servers running the same secure protocols, either RADIUS or TACACS+. Users can set these servers in a preferable order, which is called the server group list. When a user tries to access the switch, the switch will ask the first server in the server group list for authentication. If no response is received, the second server will be queried, and so on.

70.1 tacacs-server host

Description

The **tacacs-server host** command is used to configure a new TACACS+ server. To delete the specified TACACS+ server, please use **no tacacs-server host** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

tacacs-server host *ip-address* [**port** *port-id*] [**timeout** *time*] [**vrfName** *vrf-name*] [**key** { [0] *string* | 7 *encryped-string* }]

no tacacs-server host *ip-address*

Parameter

ip-address —— Specify the IP address of the TACACS+ server.

port-id —— Specify the server's port number for AAA. By default it is 49.

time —— Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

vrf-name——Specify the vrf name of the TACACS server. By the default it is default.

[0] *string* | 7 *encrypted-string* —— 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages. "*encrypted-string*" is a symmetric encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The TACACS+ servers you configured are added in the server group "tacacs" by default.

Example

Configure a TACACS+ server with the IP address as 1.1.1.1, TCP port as 1500, timeout as 6 seconds, VRF instance asv1, and the unencrypted key string as 12345.

```
Device(config)# tacacs-server host 1.1.1.1 port 1500 timeout 6 vrfName
v1 key 12345
```

70.2 show tacacs-server

Description

This **show tacacs-server** command is used to display the summary information of the TACACS+ servers.

Syntax

show tacacs-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the TACACS+ servers:

```
Device(config)# show tacacs-server
```

70.3 radius-server host

Description

The **radius-server host** command is used to configure a new RADIUS server. To delete the specified RADIUS server, please use **no radius-server host** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

radius-server host *ip-address* [**auth-port** *port-id*] [**acct-port** *port-id*] [**timeout** *time*] [**retransmit** *number*] [**nas-id** *nas-id*] [**vrfName** *vrf-name*] [**radsec-enable** *radsec-enable*] [**verify-enable** *verify-enable*] [**tls-port** *port*] [**tls-idletimeout** *idletimeout*][**tls-connectiontimeout** *connectiontimeout*] [**tls-retrys** *retrys*] [**certificate** *certificate*] [**client-profile-id** *client-profile-id*] [**key** { [0] *string* | 7 *encrypted-string* }]

no radius-server host *ip-address*

Parameter

ip-address —— Specify the IP address of the RADIUS server.

auth-port *port-id* —— Specify the UDP destination port for authentication requests. By default it is 1812.

acct-port *port-id* —— Specify the UDP destination port for accouting requests. By deault it is 1813.

time —— Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

number —— Specify the number of times a RADIUS request is resent to a server if the server is not responding in time. By default it is 2 times.

nas-id——Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

vrf-name——Specify the vrf name of the RADIUS server. By the default it is default.

radsec-enable: RADSEC state (enabled/disabled).

verify-enable: State of validating RADIUS server certificate

(enabled/disabled).

port: RADIUS server listening port, ranging from 1 to 65535.

idletimeout: TLS tunnel idle timeout, ranging from 10 to 60.

connectiontimeout: TLS connection timeout, ranging from 1 to 9.

retrys: Number of send attempts, ranging from 1 to 5.

certificate: Certificate template name.

client-profile-id: Client template name and client key

[0] *string* | 7 *encrypted-string*—— 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages. "*encrypted-string*" is a symmetric encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The RADIUS servers you configured are added in the server group "radius" by default.

Example

Configure a RADIUS server with an IP address of 1.1.1.1, an auth-port of 1200, a timeout of 6, a retransmit of 3, a VRF instance of v1, and a key of 12345.

```
Device(config)# radius-server host 1.1.1.1 auth-port 1200 timeout 6
retransmit 3 vrfName v1 key 12345
```

70.4 show radius-server

Description

This **show radius-server** command is used to display the summary information of the RADIUS servers.

Syntax

show radius-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the RADIUS servers:

```
Device(config)# show radius-server
```

70.5 show radius-server certificate

Description

This **show radius-server certificate** command is used to display the certificate directory and the corresponding certificate names.

Syntax

show radius-server certificate

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the certificate directory and corresponding certificate names:

Device(config)# show radius-server certificate

70.6 aaa group

Description

This **aaa group** command is used to create AAA server groups to group existing TACACS+/RADIUS servers for authentication. This command puts the switch in the server group subconfiguration mode.

To delete the corresponding AAA group, please use the **no aaa group** command.

Syntax

aaa group { radius | tacacs } *group-name*

no aaa group { radius | tacacs } *group-name*

Parameter

radius | tacacs —— Specify the server group type as RADIUS or TACACS+.

group-name —— Specify the server group name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a RADIUS server group with the name radius1:

Device(config)# aaa group radius radius1

70.7 server

Description

This **server** command is used to add the existing server in the defined server group. To remove the specified server from the server group, please use the **no server** command. When the command includes a VRF name, it indicates that the server address belongs to that specific VRF instance.

Syntax

server *ip-address* [**vrfName** *vrf-name*]

no server *ip-address* [**vrfName** *vrf-name*]

Parameter

ip-address —— Specify the server's IP address.

vrf-name——Specify the vrf name of the server. By the default it is default.

Command Mode

Server Group Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create the RADIUS server 1.1.1.1 and VRF address v1 to RADIUS server group "rad copy startup-config tftp command is used to backup the configuration file to TFTP server ius1":

```
Device(config)# aaa group radius radius1
Device(aaa-group)# server 1.1.1.1 vrfName v1
```

70.8 show aaa group

Description

This **show aaa group** command is used to display the summary information of the AAA groups. All the servers in this group will be listed if you specify the group name.

Syntax

show aaa group [*group-name*]

Parameter

group-name —— Specify the server group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the server groups:

```
Switch(config)# show aaa group
```

70.9 aaa authentication login

Description

This **aaa authentication login** command is used to configure a login authentication method list. A method list describes the authentication methods and their sequence to authenticate a user. To delete the specified authentication method list, please use the **no aaa authentication login** command.

Syntax

aaa authentication login { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication login *method-list*

Parameter

method-list —— Specify the method list name.

method1, method2, method3, method4 —— Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. “radius” means the RADIUS server group “radius”; “tacacs” means the RACACS+ server group “tacacs”; “local” means local username database are used; “none” means no authentication is used for login.

Users can aslo define new method with the aaa group command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the login authentication method list is “default” with “local” as method1.

Example

Configure a login authentication method list “list1” with the priority1 method as radius and priority2 method as local:

Device(config)# aaa authenticaiton login list1 radius local

70.10 aaa authentication enable

Description

This **aaa authentication enable** command is used to configure a privilege authentication method list. A method list describes the authentication methods and their sequence to elevate a user’s privilege. To delete the specified authentication method list, please use the **no aaa authentication enable** command.

Syntax

aaa authentication enable { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication enable *method-list*

Parameter

method-list —— Specify the method list name.

method1, method2, method3, method4 —— Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. “radius” means the RADIUS server group “radius”; “tacacs” means the RACACS+ server group “tacacs”; “local” means local username database are used; “none” means no authentication is used for privilege elevation.

Users can aslo define new method with the aaa group command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the enable authentication method is “default” with “none” as method1.

Example

Configuare a privilege authentication method list “list2” with the priority1 method as radius and priority2 method as local:

Device(config)# aaa authenticaiton enable list2 radius local

70.11 aaa authentication dot1x default

Description

This **aaa authentication dot1x default** command is used to configure an 802.1x authentication method list. A method list describes the authentication methods for users’ login in 802.1x. To delete the default authentication method list, please use the **no aaa authentication dot1x default** command.

Syntax

aaa authentication dot1x default { *method*}

no aaa authentication dot1x default

Parameter

method—— Specify the method name. Only RADIUS server group is supported, and the default method is server group “radius”.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1x authentication method as “radius1”:

Device(config)# aaa authentication dot1x default radius1

70.12 aaa accounting dot1x default

Description

This **aaa accounting dot1x default** command is used to configure an 802.1x accounting method list. To delete the default accounting method list, please use the **no aaa accounting dot1x default** command.

Syntax

aaa accounting dot1x default { *method*}

no aaa accounting dot1x default

Parameter

method—— Sp+ecify the method name. Only RADIUS server group is supported, and the default method is server group “radius”.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1x accounting method as “radius1”:

Device(config)# aaa accounting dot1x default radius1

70.13 show aaa authentication

Description

This **show aaa authentication** command is used to display the summary information of the authentication login, enable and dot1x metheod list.

Syntax

show aaa authentication [login | enable | dot1x]

Parameter

login | enable | dot1x —— Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the authentication method lists:

Device(config)# show aaa authentication

70.14 show aaa accounting

Description

This **show aaa accounting** command is used to display the summary information of the accounting metheod list.

Syntax

show aaa accounting [dot1x]

Parameter

dot1x —— Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the default 802.1x accounting method list:

```
Device(config)# show aaa accounting
```

70.15 line telnet

Description

The **line telnet** command is used to enter the Line Configuration Mode to configure the telnet terminal line to which you want to apply the authentication list.

Syntax

line telnet

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the telnet terminal line configuration mode:

```
Device(config)#line telnet
```

70.16 login authentication (telnet)

Description

The **login authentication** command is used to apply the login authentication method list to the telnet terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list —— Specify the login method list on the telnet terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the telnet terminal line as "list1":

```
Device(config)#line telnet
Device(config-line)# login authentication list1
```

70.17 line ssh

Description

The **line ssh** command is used to enter the Line Configuration Mode to configure the ssh terminal line to which you want to apply the authentication list.

Syntax

line ssh

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the ssh terminal line configuration mode:

```
Device(config)#line ssh
```

70.18 login authentication (ssh)

Description

The **login authentication** command is used to apply the login authentication method list to the ssh terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list —— Specify the login method list on the ssh terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the ssh terminal line as "list1":

```
Device(config)# line ssh
Device(config-line)# login authentication list1
```

70.19 line console

Description

The **line console** command is used to enter the Line Configuration Mode to configure the console terminal line to which you want to apply the authentication list.

Syntax

line console *line-number*

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the console 0 terminal line configuration mode:

```
Device(config)#line console 0
```

70.20 login authentication (console)

Description

The **login authentication** command is used to apply the login authentication method list to the console terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list —— Specify the login method list on the console terminal line. It is “default” by default, which contains the method “local”.

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the console 0 terminal line as “list1”:

Device(config)# line console 0

Device(config-line)# login authentication list1

70.21 enable authentication (telnet)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the telnet terminal line. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

enable authentication { *method-list*}

no enable authentication

Parameter

method-list —— Specify the enable method list on the telnet terminal line. It is “default” by default, which contains the method “none”.

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the telnet terminal line as “list2”:

Device(config)#line telnet

Device(config-line)# enable authentication list2

70.22 enable authentication (ssh)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the ssh terminal line. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

enable authentication { *method-list*}

no enable authentication

Parameter

method-list —— Specify the enable method list on the ssh terminal line. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the ssh terminal line as "list2":

```
Device(config)# line ssh
Device(config-line)# enable authentication list2
```

70.23 enable authentication (console)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the console terminal line. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

enable authentication { *method-list*}

no enable authentication

Parameter

method-list —— Specify the enable method list on the console terminal line. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the console 0 terminal line as "list2":

```
Device (config)# line console 0
Device(config-line)# enable authentication list2
```

70.24 ip http login authentication

Description

The **ip http login authentication** command is used to apply the login authentication method list to users accessing through HTTP. To restore to the default authentication method list, please use the **no ip http login authentication** command.

Syntax

ip http login authentication { *method-list* }

no ip http login authentication

Parameter

method-list —— Specify the login method list on the HTTP access. It is "default" by default, which contains the method "local".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the HTTP access as “list1”:

```
Device(config)# ip http login authentication list1
```

70.25 ip http enable authentication

Description

The **ip http enable authentication** command is used to apply the privilege authentication method list to users accessing through HTTP. To restore to the default authentication method list, please use the **no ip http enable authentication** command.

Syntax

ip http enable authentication { *method-list* }

no ip http enable authentication

Parameter

method-list —— Specify the enable method list on the HTTP access. It is “default” by default, which contains the method “none”.

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the HTTP access as “list2”:

```
Device(config)# ip http enable authentication list2
```

70.26 show aaa global

Description

This **show aaa global** command is used to display global status of AAA function and the login/enable method lists of different application modules: telnet, ssh and HTTP.

Syntax

show aaa global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the AAA function's global status and each application's method list:

```
Device(config)# show aaa global
```

70.27 enable admin password

Description

The **enable admin password** command is used to set or change the Enable password for users to change the access level to admin. To remove the Enable password, please use **no enable admin** command. This command uses the symmetric encryption.

Syntax

enable admin password { [0] *password* | 7 *encrypted-password*}

no enable admin

Parameter

0 —— Specify the encryption type. 0 indicates that an unencrypted password will follow. By default, the encryption type is 0.

password —— Enable password, a string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. By default, it is empty.

7 —— Indicates a symmetric encrypted password with fixed length will follow.

encrypted-password —— A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If the password you configured here is unencrypted and the global encryption function is enabled in service password-encryption, the password in the configuration file will be displayed in the symmetric encrypted form.

If both the **enable admin password** and **enable admin secret** are defined, only the latest configured password will take effect.

Example

Set the Enable password as "abc123" and unencrypted for users to change the access level to admin:

```
Device(config)#enable admin password 0 abc123
```

70.28 enable admin secret

Description

The **enable admin secret** command is used to set or change the Enable password for users to change the access level to admin. To remove the Enable password, please use **no enable admin** command. This command uses the MD5 encryption.

Syntax

enable admin secret { [0] *password* | 5 *encrypted-password* | 8 *encrypted-password* | 9 *encrypted-password*}

no enable admin

Parameter

0 ——Specify the encryption type. 0 indicates that an unencrypted password will follow. the password will be encrypted by MD5. By default, the encryption type is 0.

password ——A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are !$%'()*,-./[]_{|}. By default, it is empty.

5 —— Indicates an MD5 encrypted password with fixed length will follow.

8 —— Indicates an PBKDF2 encrypted password with fixed length will follow.

9 —— Indicates a SCRYPT encrypted password with fixed length will follow.

encrypted-password —— An/A MD5/SCRYPT/PBKDF2 encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password if you re-enter this mode.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **enable admin password** and **enable admin secret** are defined, only the latest configured password will take effect.

Example

Set the Enable password as "abc123" and unencrypted for users to change the access level to admin. The password will be displayed in the encrypted form.

```
Device(config)#enable admin secret 0 abc123
```

70.29 enable-admin

Description

The **enable-admin** command is used to get the administrative privelges by a non-admin user.

Syntax

enable-admin

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only User, Power User and Operator level users have access to these commands.

Example

Get the administrative privelges (the Enable password is “123456”):

Device# enable-admin

Password: 123456

Chapter 71 IEEE 802.1x Commands

IEEE 802.1x function is to provide an access control for LAN ports via the authentication. An 802.1x system include three entities: supplicant, authenticator and authentication server.

- Supplicant: the device that requests access to the LAN.
- Authentication server: performs the actual authentication of the supplicant. It validates the identity of the supplicant and notifies the authenticator whether or not the supplicant is authorized to access the LAN.
- Authenticator: controls the physical access to the network based on the authentication status of the supplicant. It is usually an 802.1x-supported network device, such as this TP-Link switch. It acts as an intermediary (proxy) between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant.

This chapter handles with the authentication process between the supplicant and the switch. To realize the authentication and accounting function, you should also enbable the AAA function and configure the RADIUS server. Go to Chapter 42 AAA Commands for more details.

71.1 dot1x system-auth-control

Description

The **dot1x system-auth-control** command is used to enable the IEEE 802.1x function globally. To disable the IEEE 802.1x function, please use **no dot1x system-auth-control** command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IEEE 802.1x function:

```
Device(config)#dot1x system-auth-control
```

71.2 dot1x handshake

Description

The **dot1x handshake** command is used enable the handshake feature. The handshake feature is used to detect the connection status between the TP-Link 802.1x supplicant and the switch. Please disable the handshake feature if you are using a non-TP-Link 802.1x-compliant client software. This feature is enabled by default.

Syntax

dot1x handshake

no dot1x handshake

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Disable the 802.1x handshake function:

```
Device(config)# no dot1x handshake
```

71.3 dot1x auth-protocol

Description

The **dot1x auth-protocol** command is used to configure the authentication protocol of IEEE 802.1x and the default 802.1x authentication method is “eap”. To restore to the default 802.1x authentication protocol, please use **no dot1x auth-protocol** command.

Syntax

dot1x auth-protocol { pap | eap }

no dot1x auth-protocol

Parameter

pap | eap ——Authentication protocols.

pap: EAP termination mode. IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP packets are terminated at the switch and repackaged in the Password Authentication Protocol (PAP) packets, and then transferred to the RADIUS server.

eap: EAP relay mode. IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP protocol packets with authentication data are encapsulated in the advanced protocol (such as RADIUS) packets and transmitted to the authentication server.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Authentication protocol of IEEE 802.1x as “pap”:

Device(config)#dot1x auth-protocol pap

71.4 dot1x vlan-assignment

Description

The **dot1x vlan-assignment** command is used to enable the VLAN assignment feature.To disable this feature, please use **no dot1x vlan-assignment** command.

802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated.

If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN.

If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN.

If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.

Syntax

dot1x vlan-assignment

no dot1x vlan-assignment

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the VLAN assignment feature:

```
Device(config)#dot1x vlan-assignment
```

71.5 dot1x accounting

Description

The **dot1x accounting** command is used to enable the IEEE 802.1x accounting function globally. To disable the IEEE 802.1x accounting function, please use **no dot1x accounting** command.

Syntax

dot1x accounting

no dot1x accounting

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the enable the IEEE 802.1x accounting function globally:

```
Device(config)#dot1x accounting
```

71.6 dot1x mab

Description

The **dot1x mab** command is used to enable the MAB feature on the port.To disable this feature, please use **no dot1x mab** command.

With MAB (MAC-Based Authentication Bypass) feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1x capability. For example, most printers, IP phones and fax machines do not have 802.1x capability.

Syntax

dot1x mab

no dot1x mab

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the MAB feature on the Gigabit Ethernet port 1/0/1:

```
Device(config)#interface gigabitEthernet 1/0/1
Device(config-if)#dot1x mab
```

71.7 dot1x guest-vlan

Description

The **dot1x guest-vlan** command is used to configure the Guest VLAN function on the port. To disable the Guest VLAN function, please use **no dot1x guest-vlan** command.

Syntax

dot1x guest-vlan *vid*

no dot1x guest-vlan

Parameter

vid—— The VLAN ID needed to enable the Guest VLAN function, ranging from 0 to 4094. 0 means that Guest VLAN is disabled. The supplicants in the Guest VLAN can access the specified network source.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the Guest VLAN function for VLAN 5 and set the VLAN ID as 20 on the Gigabit Ethernet port 1/0/1::

```
Device(config)#interface gigabitEthernet 1/0/1
Device(config-if)#dot1x guest-vlan 5
```

71.8 dot1x timeout quiet-period

Description

The **dot1x timeout quiet-period** command is used to enable the quiet-period function on the port. To disable the function, please use **no dot1x timeout quiet-period** command.

Syntax

dot1x timeout quiet-period [*time*]

no dot1x timeout quiet-period

Parameter

time —— The length of the quiet-period time. If one user's authentication fails, its subsequent IEEE 802.1x authentication requests will not be processed during the quiet-period time. It ranges from 1 to 999 seconds and the default value is 10 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the quiet-period function and set the quiet-period as 5 seconds on the Gigabit Ethernet port 1/0/1:

Device(config)#interface gigabitEthernet 1/0/1

Device(config-if)#dot1x quiet-period 5

71.9 dot1x timeout supp-timeout

Description

The **dot1x timeout supp-timeout** command is used to configure the supplicant timeout on the port. To restore to the default, please use **no dot1x timeout supp-timeout** command.

Syntax

dot1x timeout supp-timeout *time*

no dot1x timeout supp-timeout

Parameter

time ——The maximum time for the switch to wait for the response from supplicant before resending a request to the supplicant, ranging from 1 to 60 in second. By default, it is 30 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the supplicant timeout value as 5 seconds on the Gigabit Ethernet pot 1/0/1:

```
Device(config)#interface gigabitEthernet 1/0/1
Device(config-if)#dot1x timeout supp-timeout 5
```

71.10 dot1x max- req

Description

The **dot1x max-req** command is used to configure the maximum transfer times of the repeated authentication request when the server cannot be connected. To restore to the default value, please use **no dot1x max-req** command.

Syntax

dot1x max-req *times*

no dot1x max-req

Parameter

times —— The maximum transfer times of the repeated authentication request, ranging from 1 to 9 in times. By default, the value is 3.

Command Mode

Interface Configuration Mode

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the maximum transfer times of the repeated authentication request as 5 on the Gigabit Ethernet port 1/0/1:

```
Device(config)#interface gigabitEthernet 1/0/1
Device(config-if)#dot1x max-req 5
```

71.11 dot1x

Description

The **dot1x** command is used to enable the IEEE 802.1x function for a specified port. To disable the IEEE 802.1x function for a specified port, please use **no dot1x** command.

Syntax

dot1x

no dot1x

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Enable the IEEE 802.1x function for the Gigabit Ethernet port 1:

Device(config)#interface gigabitEthernet 1/0/1

Device(config-if)#dot1x

71.12 dot1x port-control

Description

The **dot1x port-control** command is used to configure the Control Mode of IEEE 802.1x for the specified port. By default, the control mode is “auto”. To restore to the default configuration, please use **no dot1x port-control** command.

Syntax

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

no dot1x port-control

Parameter

auto | authorized-force | unauthorized-force —— The Control Mode for the port.

auto: In this mode, the port will normally work only after passing the 802.1x Authentication.

authorized-force: In this mode, the port can work normally without passing the 802.1x Authentication.

unauthorized-force: In this mode, the port is forbidden working for its fixed unauthorized status.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Control Mode for Gigabit Ethernet port 20 as "authorized-force":

Device(config)#interface gigabitEthernet 1/0/20

Device(config-if)#dot1x port-control authorized-force

71.13 dot1x port-method

Description

The **dot1x port-method** command is used to configure the control type of IEEE 802.1x for the specified port. By default, the control type is "mac-based". To restore to the default configuration, please use **no dot1x port-method** command.

Syntax

dot1x port-method { mac-based | port-based }

no dot1x port-method

Parameter

mac-based | port-based ——The control type for the port.

mac-based: Any client connected to the port should pass the 802.1x authentication for access.

port-based: All the clients connected to the port can access the network on the condition that any one of the clients has passed the 802.1x Authentication.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin, Operator and Power User level users have access to these commands.

Example

Configure the Control Type for Gigabit Ethernet port 20 as "port-based":

Device(config)#interface gigabitEthernet 1/0/20

Device(config-if)#dot1x port-method port-based

71.14 dot1x auth-init

Description

The **dot1x auth-init** command is used to initialize the specific client.

Syntax

dot1x auth-init [mac *mac-address* **]**

Parameter

mac-address: Enter the MAC address of the client that will be unauthorized.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Initialize the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

Device(Config)# interface gigabitEthernet 1/0/1

Device(Config-if)#dot1x auth-init mac 00:02:58:4f:6c:23

71.15 dot1x auth-reauth

Description

The **dot1x auth-reauth** command is used to reauthenticate the specific client.

Syntax

dot1x auth-reauth [**mac** *mac-address*]

Parameter

mac-address: Enter the MAC address of the client that will be reauthenticated.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Reauthenticate the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

Device(Config)# interface gigabitEthernet 1/0/1

Device(Config-if)#dot1x auth-reauth mac 00:02:58:4f:6c:23

71.16 show dot1x global

Description

The **show dot1x global** command is used to display the global configuration of 801.X.

Syntax

show dot1x global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of 801.X globally:

Switch(config)#show dot1x global

71.17 show dot1x interface

Description

The **show dot1x interface** command is used to display all ports or the specified port's configuration information of 801.X.

Syntax

show dot1x interface [**gigabitEthernet** *port*]

Parameter

port —— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of 801.X for Gigabit Ethernet port 20:

```
Device(config)#show dot1x interface gigabitEthernet 1/0/20
```

Display the configuration information of 801.X for all Ethernet ports:

```
Device(config)#show dot1x interface
```

71.18 show dot1x auth-state interface

Description

The **show dot1x auth-state interface** command is used to display the authentication status of each port.

Syntax

show dot1x auth-state interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*]

Parameter

port —— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the authentication status of each port:

```
Device(config)#show dot1x auth-state interface
```

Chapter 72 Board Management Commands

This chapter introduces commands used for managing boards within the system. These commands allow users to query board information, enable or disable automatic loading, load specific boards, switch active main control boards, and lock service board traffic forwarding. They provide essential functionality for configuring, monitoring, and maintaining board operations in the device.

72.1 show board

Description

The **show board** command is used to query information about the entire frame of boards or detailed information about boards in specified slots. It is used when, after performing a certain operation on a board, you need to check details such as the slot number, name, status, daughterboard information, port information, power status, or online status of that board.

Syntax

show board { *frame-id*| *frame-id/slot-id***}**

Parameter

frame-id——Query information about all boards in a specific frame.

frame-id/slot-id——Query information about the board in a specific slot.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin

Example

Show board:

```
DS-P8000-X7_000011(active)(config)#show board fram 1 slot 4
```

72.2 board add

Description

The **board add** command is used to enable the automatic loading function for the board. After the command is successfully executed, the configuration of the board in this slot will be cleared.

Syntax

board frame *frame-id* **slot** *slot-id* **add** *board-type*

Parameter

frame-id——— Specify a frame ID.

slot-id———Specify a slot ID.

board-type——— Specify a board type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin

Example

Add the board of DS-LSGA-08 for frame 1 slot 3:

```
DS-P8000-X7_000011(active)(config)#board frame 1 slot 3 add
DS-LSGA-08
```

72.3 board auto-load

Description

The **board auto-load** command is used to enable the automatic loading function for the board. After the command is successfully executed, the automatic loading function takes effect.

Syntax

board frame *frame-id* **slot** *slot-id* **auto-load**

no board frame *frame-id* **slot** *slot-id* **auto-load**

Parameter

frame-id—— Specify a frame ID.

slot-id——Specify a slot ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin

Example

Configure auto-load for frame 1 slot 3:

```
DS-P8000-X7_000011(active)(config)#board frame 1 slot 3 auto-load
```

72.4 board delete

Description

The **board delete** command is used to enable the automatic loading function for the board. After the command is successfully executed, the configuration of the board in this slot will be cleared.

Syntax

board frame *frame-id* **slot** *slot-id* **delete**

Parameter

frame-id—— Specify a frame ID.

slot-id——Specify a slot ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin

Example

Delete a board for frame 1 slot 3:

```
DS-P8000-X7_000011(active)(config)#board frame 1 slot 3 delete
```

72.5 board load

Description

The **board load** command is used to load a board configured with "no auto-load." After successful execution of the command, the board is loaded into the system.

Syntax

board frame *frame-id* **slot** *slot-id* **load**

Parameter

frame-id—— Specify a frame ID.

slot-id——Specify a slot ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin

Example

Load a board for frame 1 slot 3:

```
DS-P8000-X7_000011(active)(config)#board frame 1 slot 3 load
```

72.6 board lock

Description

The **board lock** command is used to lock the traffic forwarding of the service board.

Syntax

board frame *frame-id* **slot** *slot-id* **lock**

Parameter

frame-id—— Specify a frame ID.

slot-id——Specify a slot ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin

Example

Lock a board for frame 1 slot 3:

```
DS-P8000-X7_000011(active)(config)#board frame 1 slot 3 lock
```

72.7 board switch-over

Description

The **board switch-over** command is used to switch the active main control board.

Syntax

board frame *frame-id* **slot** *slot-id* **switch-over**

Parameter

frame-id —— Specify a frame ID.

slot-id ——Specify a slot ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin

Example

Switch the main board for frame 1 slot 3:

```
DS-P8000-X7_000011(active)(config)#board frame 1 slot 3 switch-over
```