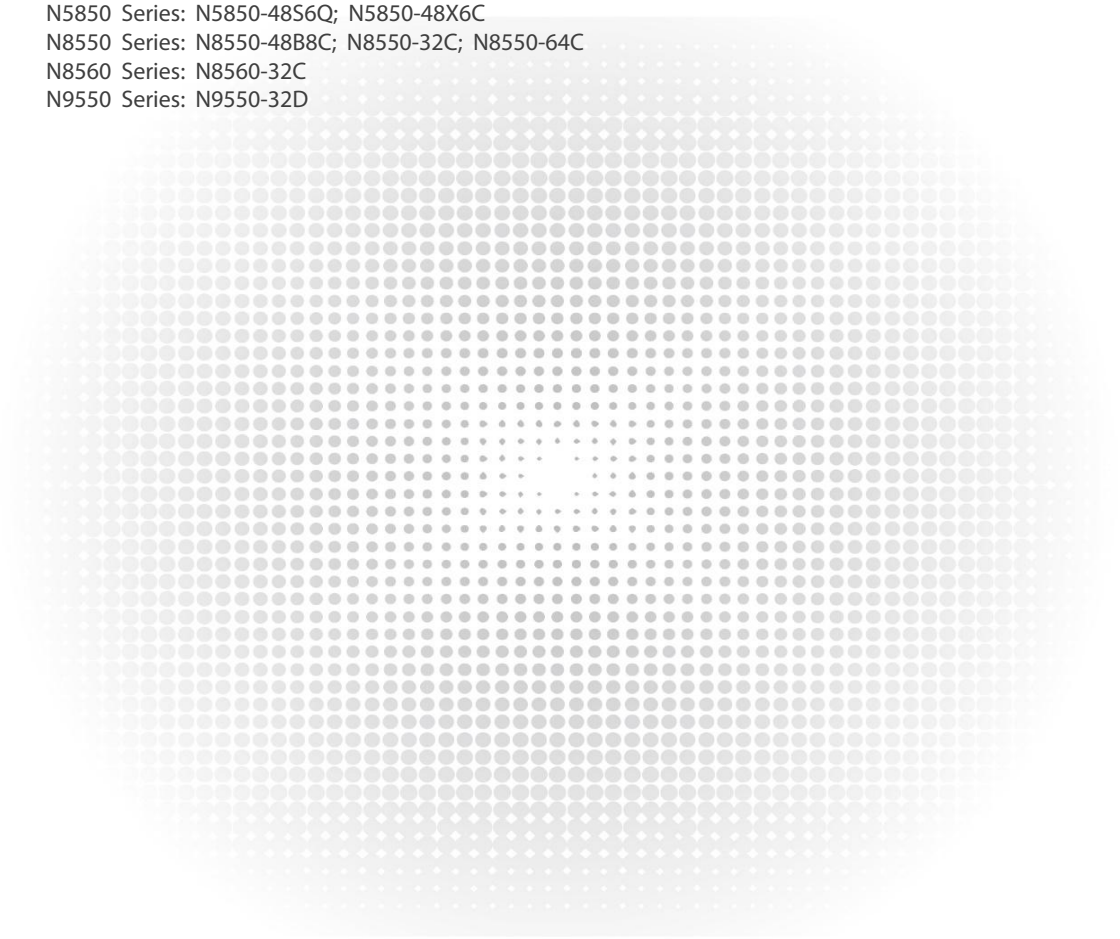
PicOS® Switches

CLI Reference Guide V4.4.5

Models:
S3410 Series: S3410L-24TF; S3410L-24TF-P; S3410-24TS; S3410-24TS-P; S3410C-16TF; S3410C-16TF-P; S3410C-16TMS-P; S3410C-8 TMS-P
S5810 Series: S5810-48TS-P; S5810-28TS; S5810-28FS; S5810-48TS; S5810-48FS
S5860 Series: S5860-20SQ; S5860-24XB-U; S5860-24MG-U; S5860-24XMG; S5860-48XMG-U; S5860-48XMG; S5860-48MG-U
S5870 Series: S5870-48T6S-U; S5870-48T6S; S5870-48T6BC-U; S5870-48T6BC; S5870-48MX6BC-U
N5850 Series: N5850-48S6Q; N5850-48X6C
N8550 Series: N8550-48B8C; N8550-32C; N8550-64C
N8560 Series: N8560-32C
N9550 Series: N9550-32D



PICOS Routing and Switching Command Reference . . . 32
Command-Line Interface Commands . . . 52
copy running-config startup-config . . . 53
set cli idle-timeout . . . 54
set cli screen-length . . . 55
set cli terminal . . . 56
syslog monitor . . . 57
syslog notify . . . 58
hwclock . . . 59
rollback . . . 61
System Management Commands . . . 62
NAC Configuration Commands . . . 66
set protocols dot1x aaa radius authentication server-ip . . . 67
set protocols dot1x aaa radius authentication server-ip priority . . . 68
set protocols dot1x aaa radius authentication server-ip retry-num . . . 69
set protocols dot1x aaa radius authentication server-ip retry-interval . . . 70
set protocols dot1x aaa radius authentication server-ip detect-interval . . . 71
set protocols dot1x interface auth-mode 802.1x . . . 72
set protocols dot1x interface auth-mode 802.1x fallback-to-web disable . . . 73
set protocols dot1x interface auth-mode mac-radius . . . 74
set protocols dot1x interface auth-mode web . . . 75
set protocols dot1x interface authentication-open disable . . . 76
set protocols dot1x aaa radius dynamic-author client . . . 77
set protocols dot1x aaa radius dynamic-author client shared-key . . . 78
set protocols dot1x aaa radius nas-ip . . . 79
set protocols dot1x aaa radius accounting disable . . . 80
set protocols dot1x interface host-mode . . . 81
set protocols dot1x block-vlan-id . . . 82
set protocols dot1x server-fail-vlan-id . . . 83
set protocols dot1x filter sequence from destination-address-ipv4 . . . 84
set protocols dot1x filter sequence from destination-address-ipv6 . . . 85
set protocols dot1x filter sequence from destination-port . . . 86
set protocols dot1x filter sequence from ether-type . . . 87
set protocols dot1x filter sequence from source-address-ipv4 . . . 88
set protocols dot1x filter sequence from source-address-ipv6 . . . 89
set protocols dot1x filter sequence from source-port . . . 90
set protocols dot1x filter sequence from protocol . . . 91
set protocols dot1x filter sequence then action . . . 92
run show dot1x all . . . 93
run show dot1x interface . . . 94
run show dot1x server . . . 96
run show dot1x dynamic filter . . . 97
run show dot1x downloadable filter . . . 98
run show dot1x interface statistics gigabit-ethernet . . . 99
set protocols dot1x server-fail recovery-method . . . 100

set protocols dot1x aaa radius authentication server-ip consecutive-detect-num . . . 101
set protocols dot1x aaa vrf mgmt-vrf . . . 102
set protocols dot1x interface session-timeout . . . 103
set protocols dot1x interface recovery-timeout . . . 104
set protocols dot1x server-fail recovery-timeout . . . 105
set protocols dot1x interface max-sessions . . . 106
set protocols dot1x max-sessions-per-port . . . 107
set protocols dot1x aaa radius authentication server-ip auth-port . . . 108
set protocols dot1x aaa radius authentication server-ip acct-port . . . 109
set protocols dot1x aaa radius dynamic-author client port . . . 110
run show dot1x radius-port . . . 111
set protocols dot1x filter sequence from destination-mac-address . . . 112
set protocols dot1x filter sequence from vlan . . . 113
SNMP Configuration Commands . . . 114
set protocols snmp trap-group targets security-name . . . 115
set protocols lldp snmp-trap . . . 116
set protocols snmp trap-group event cpu-threshold enable . . . 117
set protocols snmp trap-group event cpu-threshold high . . . 118
set protocols snmp trap-group event cpu-threshold interval . . . 119
set protocols snmp trap-group event cpu-threshold low . . . 120
set protocols snmp trap-group event mac-threshold enable . . . 121
set protocols snmp trap-group event mac-threshold interval . . . 122
set protocols snmp trap-group event mac-threshold limit . . . 123
set protocols snmp trap-group vrf mgmt-vrf . . . 124
set protocols snmp trap-group version . . . 125
set protocols snmp v3 enable . . . 126
set protocols snmp v3 usm-user . . . 127
set protocols snmp v3 usm-user group . . . 128
set protocols snmp v3 group notify-view . . . 129
set protocols snmp v3 group read-view . . . 130
set protocols snmp v3 group write-view . . . 131
set protocols snmp v3 group security-level . . . 132
set protocols snmp v3 usm-user authentication-mode . . . 133
set protocols snmp v3 usm-user authentication-key . . . 134
set protocols snmp v3 usm-user privacy-mode . . . 135
set protocols snmp v3 usm-user privacy-key . . . 136
set protocols snmp v3 mib-view subtree mask . . . 137
set protocols snmp v3 mib-view subtree type . . . 138
set protocols snmp trap-group source-interface . . . 139
set protocols snmp community . . . 140
set protocols snmp community authorization . . . 141
set protocols snmp community clients . . . 142
set protocols snmp contact . . . 143
set protocols snmp location . . . 144
run show snmp statistics . . . 145

Mirror Configuration Commands . . . 146
set interface ethernet-switching-options analyzer input . . . 147
set interface ethernet-switching-options analyzer output . . . 148
set interface ethernet-switching-options analyzer erspan input . . . 149
set interface ethernet-switching-options analyzer erspan output source-ip . . . 150
set interface ethernet-switching-options analyzer erspan output dest-ip . . . 151
set interface ethernet-switching-options analyzer erspan output vrf . . . 152
run show analyzer . . . 153
set firewall filter sequence then erspan source-ip . . . 154
set firewall filter sequence then erspan dest-ip . . . 155
set firewall filter sequence then erspan vrf . . . 156
set firewall filter sequence then erspan ttl . . . 157
RMON Commands . . . 158
run show rmon alarms . . . 159
run show rmon eventlog . . . 160
run show rmon events . . . 161
run show rmon history . . . 162
run show rmon statistics . . . 163
set protocols snmp rmon alarm falling-event-index . . . 164
set protocols snmp rmon alarm falling-threshold . . . 165
set protocols snmp rmon alarm interval . . . 166
set protocols snmp rmon alarm owner . . . 167
set protocols snmp rmon alarm rising-event-index . . . 168
set protocols snmp rmon alarm rising-threshold . . . 169
set protocols snmp rmon alarm sample-type . . . 170
set protocols snmp rmon alarm variable . . . 171
set protocols snmp rmon event community . . . 172
set protocols snmp rmon event description . . . 173
set protocols snmp rmon event owner . . . 174
set protocols snmp rmon event type . . . 175
set protocols snmp rmon history buckets . . . 176
set protocols snmp rmon history interface . . . 177
set protocols snmp rmon history interval . . . 178
set protocols snmp rmon history owner . . . 179
set protocols snmp rmon statistics interface . . . 180
set protocols snmp rmon statistics owner . . . 181
RESTCONF Commands . . . 182
set protocols restconf . . . 183
set protocols restconf port . . . 184
set protocols restconf traceoptions flag config disable . . . 185
set protocols restconf traceoptions flag all disable . . . 186
set protocols restconf traceoptions flag datastore disable . . . 187
run show system boot-messages . . . 188
run show system connections . . . 189
run show system core-dumps . . . 193

run show system cpu-usage . . . 194
run show system date . . . 195
run show system fan . . . 196
run show system memory-usage . . . 197
run show system name . . . 198
run show system ntp-status . . . 199
run show system os . . . 200
run show system processes brief . . . 201
run show system processes detail . . . 203
run show system rollback compare to . . . 205
run show system rollback file . . . 206
run show system rollback list . . . 208
run show system rpsu . . . 209
run show system serial-number . . . 210
run show system temperature . . . 211
run show system uptime . . . 212
run show system users . . . 213
set system aaa local disable . . . 214
set system aaa radius accounting disable . . . 215
set system aaa radius accounting server-ip . . . 216
set system aaa radius accounting server-ip port . . . 217
set system aaa radius accounting server-ip shared-key . . . 218
set system aaa radius accounting server-ip timeout . . . 219
set system aaa radius authorization disable . . . 220
set system aaa radius authorization server-ip . . . 221
set system aaa radius authorization server-ip port . . . 222
set system aaa radius authorization server-ip shared-key . . . 223
set system aaa radius authorization server-ip timeout . . . 224
set system aaa radius vrf mgmt-vrf . . . 225
set system aaa tacacs-plus accounting . . . 226
set system aaa tacacs-plus authorization . . . 227
set system aaa tacacs-plus auth-type . . . 228
set system aaa tacacs-plus disable . . . 229
set system aaa tacacs-plus key . . . 230
set system aaa tacacs-plus port-number . . . 231
set system aaa tacacs-plus timeout . . . 232
set system aaa tacacs-plus server-ip . . . 233
set system aaa tacacs-plus source-interface . . . 234
set system aaa local-auth-fallback disable . . . 235
set system aaa tacacs-plus vrf mgmt-vrf . . . 236
set system hostname . . . 237
set system inband vlan-interface . . . 238
set system inband loopback . . . 239
set system inband routed-interface . . . 240
set system inband enable . . . 241

system login-acl network . . . 242
system login announcement . . . 243
system login user . . . 244
system login user admin class . . . 245
set system login user authentication plain-text-password . . . 246
system login user class . . . 247
set system timezone . . . 248
set system ntp server-ip . . . 249
set system ntp source-interface . . . 250
set system ntp vrf mgmt-vrf . . . 251
set interface gigabit-ethernet ptp mode . . . 252
set system services ssh connection-limit . . . 253
set system services ssh disable . . . 254
set system services ssh protocol-version v2 . . . 255
set system services ssh rate-limit . . . 256
set system services ssh root-login . . . 257
set system services ssh idle-timeout . . . 258
set system services ssh port . . . 259
set system snmp-acl security-name network . . . 260
set system syslog server-ip . . . 261
set system syslog local-file . . . 262
set system syslog vrf mgmt-vrf . . . 263
set system usb disable . . . 264
set system management-ethernet eth0 ip-address {IPv4 | IPv6} . . . 265
set system management-ethernet eth0 ip-gateway {IPv4 | IPv6} . . . 266
show system management-ethernet . . . 267
run request system reboot . . . 268
run show system hwinfo . . . 270
ping . . . 271
traceroute . . . 273
tftp . . . 274
set protocols sflow collector vrf mgmt-vrf . . . 275
scp . . . 276
set system login banner . . . 277
upgrade2 image-file . . . 278
upgrade2 image-file backup-file . . . 279
upgrade2 image-file factory-default . . . 281
upgrade2 image-file use-prev-config . . . 282
set system dns-server-ip . . . 283
set system console idle-timeout . . . 284
set system login multiline-banner message . . . 285
set system login multiline-announcement message . . . 286
set system aaa radius source-interface . . . 287
set protocols grpc enable . . . 288
set protocols grpc port . . . 289

set system ztp enable . . . 290
telnet . . . 291
set system start-shell-sh password . . . 293
set system services telnet disable . . . 294
Interface Configuration Commands . . . 295
Port Security Commands . . . 298
set interface gigabit-ethernet port-security mac-address vlan . . . 299
set interface gigabit-ethernet port-security mac-limit . . . 300
set interface gigabit-ethernet port-security sticky . . . 301
set interface gigabit-ethernet port-security violation . . . 302
set interface gigabit-ethernet port-security block . . . 303
set interface ethernet-switching-options port-error-discard timeout . . . 304
run show port-security brief . . . 305
run show port-security address . . . 306
run show port-security interface . . . 307
run clear port-security port-error . . . 309
run clear port-security sticky interface . . . 310
run clear port-security sticky address . . . 311
run clear port-security dynamic interface . . . 312
run clear port-security dynamic address . . . 313
L3 Interface . . . 314
set l3-interface vlan-interface vrf . . . 315
set l3-interface vlan-interface address prefix-length . . . 316
set l3-interface loopback address . . . 317
set l3-interface loopback disable . . . 318
set l3-interface loopback vrf . . . 319
set l3-interface vlan-interface rate-limit . . . 320
set l3-interface vlan-interface mtu . . . 321
set l3-interface vlan-interface dhcp . . . 322
run show l3-interface vlan-interface . . . 323
run show l3-interface . . . 324
run show l3-interface loopback . . . 326
run clear l3-interface statistics . . . 327
set l3-interface routed-interface dhcp . . . 328
set l3-interface routed-interface rate-limit . . . 329
set l3-interface routed-interface mtu . . . 330
set l3-interface routed-interface vrf . . . 331
set l3-interface routed-interface address . . . 332
set l3-interface routed-interface description . . . 333
run show l3-interface routed-interface . . . 334
set l3-interface vlan-interface pmtu-discovery . . . 335
set l3-interface routed-interface pmtu-discovery . . . 336
Routed Interface . . . 337
run show interface routed-interface brief . . . 338
run show vlans routed-vlan . . . 339

set interface aggregate-ethernet routed-interface enable . . . 340
set interface aggregate-ethernet routed-interface name . . . 341
set interface aggregate-ethernet routed-interface sub-interface vlan-id . . . 342
set interface gigabit-ethernet routed-interface enable . . . 343
set interface gigabit-ethernet routed-interface sub-interface . . . 345
set vlans reserved-vlan . . . 346
set interface gigabit-ethernet routed-interface name . . . 348
Uplink Failure Detection Commands . . . 349
run show interface ufd . . . 350
set interface ufd link-to-monitor . . . 351
set interface ufd link-to-disable . . . 352
IPv6 Neighbor Discovery Protocol Command Reference . . . 353
set l3-interface routed-interface ipv6-nd adv-interval-option . . . 354
set l3-interface routed-interface ipv6-nd home-agent-config-flag . . . 355
set l3-interface routed-interface ipv6-nd home-agent-lifetime . . . 356
set l3-interface routed-interface ipv6-nd home-agent-preference . . . 357
set l3-interface routed-interface ipv6-nd managed-config-flag . . . 358
set l3-interface routed-interface ipv6-nd mtu . . . 359
set l3-interface routed-interface ipv6-nd other-config-flag . . . 360
set l3-interface routed-interface ipv6-nd prefix off-link . . . 361
set l3-interface routed-interface ipv6-nd prefix preferred-lifetime . . . 362
set l3-interface routed-interface ipv6-nd prefix router-address . . . 363
set l3-interface routed-interface ipv6-nd prefix valid-lifetime . . . 364
set l3-interface routed-interface ipv6-nd ra-fast-retrans . . . 365
set l3-interface routed-interface ipv6-nd ra-interval . . . 366
set l3-interface routed-interface ipv6-nd ra-lifetime . . . 367
set l3-interface routed-interface ipv6-nd reachable-time . . . 368
set l3-interface routed-interface ipv6-nd router-preference . . . 369
set l3-interface routed-interface ipv6-nd suppress-ra . . . 370
set l3-interface vlan-interface ipv6-nd adv-interval-option . . . 371
set l3-interface vlan-interface ipv6-nd home-agent-config-flag . . . 372
set l3-interface vlan-interface ipv6-nd home-agent-lifetime . . . 373
set l3-interface vlan-interface ipv6-nd home-agent-preference . . . 374
set l3-interface vlan-interface ipv6-nd managed-config-flag . . . 375
set l3-interface vlan-interface ipv6-nd mtu . . . 376
set l3-interface vlan-interface ipv6-nd other-config-flag . . . 377
set l3-interface vlan-interface ipv6-nd prefix off-link . . . 378
set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime . . . 379
set l3-interface vlan-interface ipv6-nd prefix router-address . . . 380
set l3-interface vlan-interface ipv6-nd prefix valid-lifetime . . . 381
set l3-interface vlan-interface ipv6-nd ra-fast-retrans . . . 382
set l3-interface vlan-interface ipv6-nd ra-interval . . . 383
set l3-interface vlan-interface ipv6-nd ra-lifetime . . . 384
set l3-interface vlan-interface ipv6-nd reachable-time . . . 385
set l3-interface vlan-interface ipv6-nd router-preference . . . 386

set l3-interface vlan-interface ipv6-nd suppress-ra . . . 387
set management-ethernet-speed eth0 . . . 388
set interface gigabit-ethernet up-mode . . . 389
set interface gigabit-ethernet speed . . . 390
show interface bpdu-tunneling . . . 391
show interface aggregate-ethernet <lag_name> . . . 392
show interface aggregate-ethernet <lag_name> dot1q-tunneling . . . 393
show interface brief . . . 394
show interface detail . . . 396
show interface diagnostics optics all . . . 397
show interface ecmp max-path . . . 398
show interface flexlink . . . 399
show interface gigabit-ethernet <interface> . . . 400
set interface gigabit-ethernet fec . . . 402
set interface gigabit-ethernet family ethernet-switching vlan members . . . 403
set interface gigabit-ethernet family ethernet-switching port-mode . . . 404
set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol . . . 406
set interface gigabit-ethernet ether-options 802.3ad . . . 407
set interface gigabit-ethernet duplex auto . . . 408
set interface gigabit-ethernet cdr . . . 409
set interface gigabit-ethernet breakout . . . 410
set interface gigabit-ethernet auto-speeds . . . 411
set interface ecmp hash-mapping field vlan disable . . . 412
set interface ecmp hash-mapping field port-source disable . . . 413
set interface ecmp hash-mapping field port-destination disable . . . 414
set interface ecmp hash-mapping field ip-source disable . . . 415
set interface ecmp hash-mapping field ip-protocol disable . . . 416
set interface ecmp hash-mapping field ip-destination disable . . . 417
set interface ecmp hash-mapping field ingress-interface disable . . . 418
set interface bpdu-tunneling destination-mac . . . 419
set interface aggregate-ethernet family ethernet-switching vlan members . . . 420
set interface aggregate-ethernet family ethernet-switching port-mode . . . 421
set interface aggregate-ethernet disable . . . 423
set interface aggregate-ethernet description . . . 424
set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout . . . 425
set interface aggregate-ethernet aggregated-ether-options lacp fallback enable . . . 426
set interface aggregate-ethernet aggregated-ether-options lacp . . . 427
set interface aggregate-ethernet . . . 428
run show interface port-index-mapping . . . 429
run show interface diagnostics tdr . . . 431
interface max-route-limit . . . 432
interface max-acl-rule-limit <egress/ingress> . . . 433
interface gigabit-ethernet <port> wred queue <value> min_thresh . . . 434
interface gigabit-ethernet <port> wred queue <value> max_thresh . . . 435
interface gigabit-ethernet <port> wred queue <value> enable . . . 436

interface gigabit-ethernet <port> wred queue <value> ecn_thresh . . . 437
interface gigabit-ethernet <port> wred queue <value> drop_probability . . . 438
interface gigabit-ethernet <port> storm-control <mode> ratio <value> . . . 439
interface gigabit-ethernet <port> storm-control <mode> pps . . . 440
interface gigabit-ethernet <port> storm-control <mode> kbps . . . 441
interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id> . . . 442
interface gigabit-ethernet <port> snmp-trap . . . 443
interface gigabit-ethernet <port> power-preemphasis-level . . . 444
interface gigabit-ethernet <port> mtu . . . 445
interface gigabit-ethernet <port> mac-learning <boolean> . . . 446
interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean> . . . 447
interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean> . . . 448
interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged . . . 449
interface gigabit-ethernet <port> family ethernet-switching native-vlan-id . . . 450
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode . . . 451
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress . . . 452
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type . . . 453
interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress . . . 454
interface gigabit-ethernet <port> disable . . . 455
interface gigabit-ethernet <port> ether-options flow-control . . . 456
interface gigabit-ethernet <port> description . . . 457
interface gigabit-ethernet <port> crossflow local-control . . . 458
interface gigabit-ethernet <port> crossflow enable . . . 459
interface gigabit-ethernet <port> backup-port mode . . . 460
interface gigabit-ethernet <port> backup-port interface . . . 461
interface gigabit-ethernet <port> backup-port delay . . . 462
interface ethernet-switching-options mac-table-aging-time . . . 463
interface ethernet-switching-options buffer queue-limit . . . 464
interface ecmp max-path . . . 465
interface cut-through-mode . . . 466
interface aggregate-ethernet <lag_name> storm-control <mode> pps . . . 467
interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan . . . 468
interface aggregate-ethernet <lag_name> snmp-trap . . . 469
interface aggregate-ethernet <lag_name> mtu . . . 470
interface aggregate-ethernet <lag_name> hash-mapping mode . . . 471
interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id . . . 472
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode . . . 473
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress . . . 474
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type . . . 475
interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress . . . 476
interface aggregate-ethernet <lag_name> crossflow local-control . . . 477
interface aggregate-ethernet <lag_name> crossflow enable . . . 478
interface aggregate-ethernet <lag_name> backup-port mode . . . 479
interface aggregate-ethernet <lag_name> backup-port interface . . . 480
interface aggregate-ethernet <lag_name> backup-port delay . . . 481

interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port . . . 482
interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control . . . 483
interface aggregate-balancing hash-mapping field vlan disable . . . 484
interface aggregate-balancing hash-mapping field port-source disable . . . 485
interface aggregate-balancing hash-mapping field port-destination disable . . . 486
interface aggregate-balancing hash-mapping field ip-source disable . . . 487
interface aggregate-balancing hash-mapping field ip-protocol disable . . . 488
interface aggregate-balancing hash-mapping field ip-destination disable . . . 489
interface aggregate-balancing hash-mapping field ingress-interface disable . . . 490
interface aggregate-balancing hash-mapping field ethernet-type disable . . . 491
interface aggregate-balancing hash-mapping field ethernet-source-address disable . . . 492
interface aggregate-balancing hash-mapping field ethernet-destination-address disable . . . 493
set interface ecmp hash-mapping randomized-load-balancing . . . 494
set interface ecmp hash-mapping round-robin-load-balancing . . . 495
set interface ecmp hash-mapping dlb-normal . . . 496
set interface ecmp hash-mapping symmetric . . . 497
VLAN Configuration Commands . . . 498
set vlans dot1q-tunneling egress from . . . 499
set vlans dot1q-tunneling egress then action . . . 500
set vlans dot1q-tunneling egress then service-vlan . . . 501
set vlans dot1q-tunneling ingress from double-tag service-vlan . . . 502
set vlans dot1q-tunneling ingress from one-tag customer-vlan-list . . . 503
set vlans dot1q-tunneling ingress from untag enabled . . . 504
set vlans dot1q-tunneling ingress then . . . 505
set vlans vlan-id . . . 506
set vlans vlan-id description . . . 507
set vlans vlan-id l3-interface . . . 508
set vlans vlan-id vlan-name . . . 509
set vlans vlan-id private-vlan mode . . . 510
set vlans vlan-id private-vlan association . . . 511
set mac-map mac-address vlan . . . 512
run show vlans . . . 513
run show vlans private-vlan . . . 514
run show vlans private-vlan type . . . 515
run show mac-map . . . 516
set tracemac disable . . . 517
tracemac . . . 518
Voice VLAN Configuration Commands . . . 519
set interface gigabit-ethernet voice-vlan mode . . . 520
set interface gigabit-ethernet voice-vlan tagged mode . . . 521
set interface gigabit-ethernet voice-vlan vlan-id . . . 522
set vlans voice-vlan aging . . . 523
set vlans voice-vlan dscp . . . 524
set vlans voice-vlan local-priority . . . 525
set vlans voice-vlan mac-address mask . . . 526

set vlans voice-vlan mac-address description . . . 527
show vlans voice-vlan . . . 528
show vlans voice-vlan oui . . . 530
show vlans voice-vlan vlan-id <text> . . . 531
Layer 3 Routing Commands . . . 532
run show neighbors . . . 538
run show route . . . 539
run show route forward-host . . . 541
run show route forward-route . . . 542
run show vrf . . . 543
set ip vrf . . . 544
set ip routing enable . . . 545
set system management-vrf enable . . . 546
BGP Commands . . . 547
run show bgp . . . 549
run show bgp neighbor . . . 550
run show bgp route . . . 553
run show bgp unicast neighbor graceful-restart . . . 554
set protocols bgp aggregate-address . . . 555
set protocols bgp always-compare-med . . . 556
set protocols bgp bestpath as-path type multipath-relax . . . 557
set protocols bgp bestpath bandwidth . . . 558
set protocols bgp bestpath compare-routerid . . . 559
set protocols bgp bestpath med missing-as-worst . . . 560
set protocols bgp cluster-id . . . 561
set protocols bgp graceful-shutdown . . . 562
set protocols bgp listen . . . 563
set protocols bgp local-as . . . 564
set protocols bgp max-med . . . 565
set protocols bgp multipath maximum-paths . . . 566
set protocols bgp neighbor activate . . . 567
set protocols bgp neighbor addpath-tx-all-paths . . . 568
set protocols bgp neighbor addpath-tx-bestpath-per-as . . . 569
set protocols bgp neighbor advertisement-interval . . . 570
set protocols bgp neighbor allowas-in . . . 571
set protocols bgp neighbor as-override . . . 572
set protocols bgp neighbor capability extended-nexthop . . . 573
set protocols bgp neighbor default-originate . . . 574
set protocols bgp neighbor description . . . 575
set protocols bgp neighbor disable-connected-check . . . 576
set protocols bgp neighbor ebgp-multihop . . . 577
set protocols bgp neighbor filter-list . . . 578
set protocols bgp neighbor next-hop-self . . . 579
set protocols bgp neighbor password . . . 580
set protocols bgp neighbor peer-group . . . 581

set protocols bgp neighbor prefix-list . . . 582
set protocols bgp neighbor remote-as . . . 583
set protocols bgp neighbor remove-private-as . . . 584
set protocols bgp neighbor route-map . . . 585
set protocols bgp neighbor route-reflector-client . . . 586
set protocols bgp neighbor send-community . . . 587
set protocols bgp neighbor shutdown . . . 588
set protocols bgp neighbor soft-reconfiguration . . . 589
set protocols bgp neighbor timers connect . . . 590
set protocols bgp neighbor timers holdtime . . . 591
set protocols bgp neighbor timers keepalive . . . 592
set protocols bgp neighbor ttl-security hops . . . 593
set protocols bgp neighbor update-source . . . 594
set protocols bgp network . . . 595
set protocols bgp network-import-check . . . 596
set protocols bgp peer-group . . . 597
set protocols bgp redistribute . . . 598
set protocols bgp route-map delay-timer . . . 599
set protocols bgp router-id . . . 600
set protocols bgp table-map . . . 601
set protocols bgp timers . . . 602
set protocols bgp update-delay . . . 603
set protocols bgp ebgp-requires-policy . . . 604
set protocols bgp neighbor timers delayopen . . . 606
set protocols bgp neighbor maximum-prefix . . . 607
set protocols bgp neighbor maximum-prefix-out . . . 608
set protocols bgp neighbor port . . . 609
set protocols bgp neighbor sender-as-path-loop-detection . . . 610
set protocols bgp fast-external-failover . . . 611
set protocols bgp confederation identifier . . . 612
set protocols bgp confederation peers . . . 613
set protocols bgp dampening . . . 614
set protocols bgp default local-preference . . . 615
set protocols bgp as-notation . . . 616
set protocols bgp neighbor local-as . . . 617
OSPFv2 Commands . . . 619
run clear ospf interface . . . 621
run show ospf border-routers . . . 622
run show ospf database . . . 623
run show ospf interface . . . 625
run show ospf neighbor . . . 626
run show ospf route . . . 628
run show ospf summary-address . . . 629
set protocols ospf aggregation timer . . . 630
set protocols ospf area area-type . . . 631

set protocols ospf area filter-list prefix . . . 632
set protocols ospf area no-summary . . . 633
set protocols ospf area range . . . 634
set protocols ospf area virtual-link . . . 635
set protocols ospf area virtual-link authentication . . . 636
set protocols ospf area virtual-link authentication-key . . . 637
set protocols ospf area virtual-link dead-interval . . . 638
set protocols ospf area virtual-link hello-interval . . . 639
set protocols ospf area virtual-link message-digest-key md5 . . . 640
set protocols ospf area virtual-link retransmit-interval . . . 641
set protocols ospf area virtual-link transmit-delay . . . 642
set protocols ospf auto-cost reference-bandwidth . . . 643
set protocols ospf compatible rfc1583 . . . 644
set protocols ospf default-information originate . . . 645
set protocols ospf default-metric . . . 646
set protocols ospf interface area . . . 647
set protocols ospf interface authentication-key . . . 648
set protocols ospf interface authentication message-digest . . . 649
set protocols ospf interface cost . . . 650
set protocols ospf interface dead-interval . . . 651
set protocols ospf interface hello-interval . . . 652
set protocols ospf interface message-digest-key md5 . . . 653
set protocols ospf interface network . . . 654
set protocols ospf interface priority . . . 655
set protocols ospf interface retransmit-interval . . . 656
set protocols ospf interface transmit-delay . . . 657
set protocols ospf log-adjacency-changes . . . 658
set protocols ospf max-metric router-lsa administrative . . . 659
set protocols ospf max-metric router-lsa on-shutdown . . . 661
set protocols ospf max-metric router-lsa on-startup . . . 663
set protocols ospf multi-instance disable . . . 665
set protocols ospf network area . . . 666
set protocols ospf passive-interface . . . 667
set protocols ospf redistribute . . . 668
set protocols ospf redistribute metric-type . . . 669
set protocols ospf redistribute route-map . . . 670
set protocols ospf router-id . . . 671
set protocols ospf summary-address . . . 672
set protocols ospf timers lsa min-arrival . . . 673
set protocols ospf timers throttle spf . . . 674
set protocols ospf traceoption ism . . . 675
set protocols ospf traceoption lsa . . . 676
set protocols ospf traceoption nsm . . . 677
set protocols ospf traceoption packet . . . 678
set protocols ospf traceoption zebra . . . 679

set protocols ospf graceful-restart enable . . . 680
set protocols ospf capability opaque . . . 681
set protocols ospf graceful-restart grace-period . . . 682
set protocols ospf graceful-restart helper enable . . . 683
set protocols ospf graceful-restart helper planned-only . . . 684
set protocols ospf graceful-restart helper strict-lsa-checking . . . 685
set protocols ospf graceful-restart helper supported-grace-time . . . 686
run graceful-restart prepare ospf . . . 687
run show ospf graceful-restart helper . . . 688
OSPFv3 Command Reference . . . 689
set protocols ospf6 area . . . 690
set protocols ospf6 area range . . . 691
set protocols ospf6 area stub . . . 692
set protocols ospf6 area stub no-summary . . . 693
set protocols ospf6 auto-cost reference-bandwidth . . . 694
set protocols ospf6 distance . . . 695
set protocols ospf6 distance-ospf6 . . . 696
set protocols ospf6 interface area . . . 697
set protocols ospf6 interface cost . . . 698
set protocols ospf6 interface dead-interval . . . 699
set protocols ospf6 interface hello-interval . . . 700
set protocols ospf6 interface ifmtu . . . 701
set protocols ospf6 interface mtu-ignore . . . 702
set protocols ospf6 interface network . . . 703
set protocols ospf6 interface passive . . . 704
set protocols ospf6 interface priority . . . 705
set protocols ospf6 interface retransmit-interval . . . 706
set protocols ospf6 interface transmit-delay . . . 707
set protocols ospf6 log-adjacency-changes . . . 708
set protocols ospf6 redistribute . . . 709
set protocols ospf6 router-id . . . 710
set protocols ospf6 stub-router administrative . . . 711
set protocols ospf6 timers lsa min-arrival . . . 712
set protocols ospf6 timers throttle spf . . . 713
set protocols ospf6 traceoption . . . 714
set protocols ospf6 traceoption border-routers . . . 715
set protocols ospf6 traceoption lsa . . . 716
set protocols ospf6 traceoption message . . . 717
set protocols ospf6 traceoption neighbor . . . 718
set protocols ospf6 traceoption route . . . 719
set protocols ospf6 traceoption spf . . . 720
set protocols ospf6 traceoption zebra . . . 721
set protocols ospf6 graceful-restart enable . . . 722
set protocols ospf6 capability opaque . . . 723
set protocols ospf6 graceful-restart grace-period . . . 724

set protocols ospf6 graceful-restart helper enable . . . 725
set protocols ospf6 graceful-restart helper planned-only . . . 726
set protocols ospf6 graceful-restart helper lsa-checking-disable . . . 727
set protocols ospf6 graceful-restart helper supported-grace-time . . . 728
run graceful-restart prepare ospf6 . . . 729
run show ospf6 graceful-restart helper . . . 730
Static Route Configuration Commands . . . 731
set protocols static interface-route interface . . . 732
set protocols static mroute . . . 733
set protocols static route . . . 734
Route Map Commands . . . 735
run show routing route-map . . . 737
set routing as-path-list . . . 738
set routing large-community-list expanded . . . 739
set routing large-community-list standard . . . 740
set routing prefix-list . . . 741
set routing prefix-list description . . . 743
set routing community-list expanded . . . 744
set routing community-list standard . . . 745
set routing extcommunity-list expanded . . . 746
set routing extcommunity-list standard . . . 747
set routing route-map set-action large-community . . . 748
set routing route-map call . . . 749
set routing route-map description . . . 750
set routing route-map match as-path . . . 751
set routing route-map match community . . . 752
set routing route-map match community-with-exact-match . . . 753
set routing route-map match evpn default-route . . . 754
set routing route-map match evpn route-type . . . 755
set routing route-map match evpn vni . . . 756
set routing route-map match extcommunity . . . 757
set routing route-map matching-policy . . . 758
set routing route-map match interface . . . 759
set routing route-map match ipv4-addr address . . . 760
set routing route-map match ipv4-addr next-hop . . . 761
set routing route-map match ipv4-addr route-source . . . 762
set routing route-map match ipv6-addr . . . 763
set routing route-map match large-community . . . 764
set routing route-map match local-preference . . . 765
set routing route-map match metric . . . 766
set routing route-map match origin . . . 767
set routing route-map match peer . . . 768
set routing route-map match source-protocol . . . 769
set routing route-map match source-vrf . . . 770
set routing route-map match tag . . . 771

set routing route-map on-match . . . 772
set routing route-map set-action aggregator . . . 773
set routing route-map set-action as-path exclude . . . 774
set routing route-map set-action as-path prepend . . . 775
set routing route-map set-action atomic-aggregate . . . 776
set routing route-map set-action comm-list-delete . . . 777
set routing route-map set-action community . . . 778
set routing route-map set-action community-additive . . . 779
set routing route-map set-action extcommunity . . . 780
set routing route-map set-action extcommunity bandwidth . . . 781
set routing route-map set-action extcommunity bandwidth-non-transitive . . . 782
set routing route-map set-action ip-next-hop . . . 783
set routing route-map set-action ipv4-vpn-next-hop . . . 784
set routing route-map set-action ipv6-next-hop . . . 785
set routing route-map set-action label-index . . . 786
set routing route-map set-action large-comm-list-delete . . . 787
set routing route-map set-action local-preference . . . 788
set routing route-map set-action metric . . . 789
set routing route-map set-action metric-type . . . 790
set routing route-map set-action origin . . . 791
set routing route-map set-action originator-id . . . 792
set routing route-map set-action src . . . 793
set routing route-map set-action tag . . . 794
set routing route-map set-action weight . . . 795
Route Leaking Commands . . . 796
BGP Route Leaking Commands . . . 797
set protocols bgp ipv4-unicast import vrf . . . 798
set protocols bgp ipv6-unicast import vrf . . . 799
set protocols bgp ipv6-unicast import vrf-route-map . . . 800
set protocols bgp vrf ipv4-unicast import vrf . . . 801
set protocols bgp vrf ipv4-unicast import vrf-route-map . . . 802
set protocols bgp vrf ipv6-unicast import vrf . . . 803
Static Route Leaking Commands . . . 804
set protocols static route nexthop-vrf next-hop . . . 805
set protocols static vrf route nexthop-vrf next-hop . . . 806
BFD Configuration Commands . . . 807
run show bfd . . . 808
run show bfd counters . . . 811
run show bfd peers . . . 812
set protocols bfd multihop peer local-address . . . 814
set protocols bfd multihop peer local-address detect-multiplier . . . 815
set protocols bfd multihop peer local-address minimum-ttl . . . 816
set protocols bfd multihop peer local-address passive-mode . . . 817
set protocols bfd multihop peer local-address receive-interval . . . 818
set protocols bfd multihop peer local-address shutdown . . . 819

set protocols bfd multihop peer local-address transmit-interval . . . 820
set protocols bfd peer detect-multiplier . . . 821
set protocols bfd peer echo-mode . . . 822
set protocols bfd peer echo receive-interval . . . 823
set protocols bfd peer echo transmit-interval . . . 824
set protocols bfd peer local-address . . . 825
set protocols bfd peer minimum-ttl . . . 826
set protocols bfd peer passive-mode . . . 827
set protocols bfd peer receive-interval . . . 828
set protocols bfd peer shutdown . . . 829
set protocols bfd peer transmit-interval . . . 830
set protocols bfd profile . . . 831
set protocols bfd profile detect-multiplier . . . 832
set protocols bfd profile echo-mode . . . 833
set protocols bfd profile echo receive-interval . . . 834
set protocols bfd profile echo transmit-interval . . . 835
set protocols bfd profile minimum-ttl . . . 836
set protocols bfd profile passive-mode . . . 837
set protocols bfd profile receive-interval . . . 838
set protocols bfd profile shutdown . . . 839
set protocols bfd profile transmit-interval . . . 840
set protocols bgp bfd . . . 841
set protocols ospf6 interface bfd . . . 842
set protocols ospf interface bfd . . . 843
set protocols pim interface bfd . . . 844
Policy-Based Routing (PBR) Commands . . . 845
set routing pbr map sequence match destination-ipv4 . . . 846
set routing pbr map sequence match source-ipv4 . . . 847
set routing pbr map sequence match destination-port . . . 848
set routing pbr map sequence match source-port . . . 849
set routing pbr map sequence match destination-ipv6 . . . 850
set routing pbr map sequence match source-ipv6 . . . 851
set routing pbr map sequence action nexthop . . . 852
set routing pbr map sequence action dscp . . . 853
set routing pbr map vlan-interface . . . 854
run show pbr map . . . 855
run clear pbr map . . . 856
IPv4 Source Guard (IPSG for IPv4) Commands . . . 857
set ip-source-guard binding ip . . . 858
set ip-source-guard enable . . . 860
set ip-source-guard verify . . . 862
set ip-source-guard traceoptions enable . . . 863
run show ip-source-guard binding . . . 864
IPv6 Source Guard (IPSG for IPv6) Commands . . . 865
set ipv6-source-guard binding ip . . . 866

set ipv6-source-guard enable . . . 868
set ipv6-source-guard verify . . . 870
set ipv6-source-guard traceoptions enable . . . 871
run show ipv6-source-guard binding . . . 872
IS-IS commands . . . 873
set protocols isis area-tag network-entity . . . 875
set protocols isis area-tag is-type . . . 877
set protocols isis area-tag interface . . . 878
set protocols isis area-tag hostname-dynamic . . . 879
set protocols isis area-tag area-password authentication-type . . . 880
set protocols isis area-tag area-password authentication-key . . . 881
set protocols isis area-tag area-password authenticate-snp . . . 882
set protocols isis area-tag domain-password authentication-type . . . 883
set protocols isis area-tag domain-password authentication-key . . . 884
set protocols isis area-tag domain-password authenticate-snp . . . 885
set protocols isis area-tag attached-bit receive-ignore . . . 886
set protocols isis area-tag attached-bit send . . . 887
set protocols isis area-tag log-adjacency-changes . . . 888
set protocols isis area-tag metric-style . . . 889
set protocols isis area-tag set-overload-bit . . . 891
set protocols isis area-tag purge-originator . . . 892
set protocols isis area-tag lsp-mtu . . . 894
set protocols isis area-tag lsp-timers gen-interval . . . 895
set protocols isis area-tag lsp-timers refresh-interval . . . 896
set protocols isis area-tag lsp-timers max-lifetime . . . 897
set protocols isis area-tag spf-interval . . . 898
set protocols isis area-tag spf-delay-ietf init-delay . . . 899
set protocols isis area-tag spf-delay-ietf short-delay . . . 901
set protocols isis area-tag spf-delay-ietf long-delay . . . 903
set protocols isis area-tag spf-delay-ietf holddown . . . 905
set protocols isis area-tag spf-delay-ietf time-to-learn . . . 906
set protocols isis area-tag default-information originate . . . 907
set protocols isis area-tag default-information originate metric . . . 908
set protocols isis area-tag default-information originate route-map . . . 909
set protocols isis area-tag topology ipv6-unicast . . . 910
set protocols isis area-tag interface circuit-type . . . 911
set protocols isis area-tag interface csnp-interval . . . 912
set protocols isis area-tag interface psnp-interval . . . 913
set protocols isis area-tag interface hello-padding . . . 914
set protocols isis area-tag interface hello-interval . . . 915
set protocols isis area-tag interface hello-multiplier . . . 916
set protocols isis area-tag interface metric . . . 917
set protocols isis area-tag interface network point-to-point . . . 918
set protocols isis area-tag interface passive . . . 919
set protocols isis area-tag interface password authentication-type . . . 920

set protocols isis area-tag interface password authentication-key . . . 921
set protocols isis area-tag interface priority . . . 922
set protocols isis area-tag interface three-way-handshake . . . 923
set protocols isis area-tag interface bfd . . . 924
set protocols isis area-tag interface topology ipv6-unicast . . . 925
set protocols isis area-tag redistribute . . . 926
set protocols isis traceoption events . . . 928
set protocols isis traceoption adj-packets . . . 929
set protocols isis traceoption route-events . . . 930
set protocols isis traceoption snp-packets . . . 931
run show isis summary . . . 932
run show isis interface . . . 933
run show isis database . . . 934
run show isis hostname . . . 936
run show isis neighbor . . . 937
run show isis route . . . 939
run show isis topology . . . 941
ACL Configuration Commands . . . 943
set firewall filter description . . . 944
set firewall filter input interface . . . 945
set firewall filter input vlan-interface . . . 946
set firewall filter input routed-interface . . . 947
set firewall filter output interface . . . 948
set firewall filter output vlan-interface . . . 949
set firewall filter output routed-interface . . . 950
set firewall filter sequence description . . . 951
set firewall filter sequence from destination-address-ipv4 . . . 952
set firewall filter sequence from destination-address-ipv6 . . . 953
set firewall filter sequence from destination-mac-address . . . 954
set firewall filter sequence from destination-port . . . 955
set firewall filter sequence from ether-type . . . 956
set firewall filter sequence from ip trust-mode . . . 957
set firewall filter sequence from ip value . . . 958
set firewall filter sequence from protocol icmp . . . 959
set firewall filter sequence from protocol igmp . . . 960
set firewall filter sequence from protocol ip . . . 961
set firewall filter sequence from protocol ospf . . . 962
set firewall filter sequence from protocol others . . . 963
set firewall filter sequence from protocol tcp . . . 964
set firewall filter sequence from protocol tcp flags . . . 965
set firewall filter sequence from protocol udp . . . 966
set firewall filter sequence from source-address-ipv4 . . . 967
set firewall filter sequence from source-address-ipv6 . . . 968
set firewall filter sequence from source-mac-address . . . 969
set firewall filter sequence from source-port . . . 970

set firewall filter sequence from vlan . . . 971
set firewall filter sequence then action . . . 972
set firewall filter sequence then forwarding-class . . . 973
set firewall filter sequence log interval . . . 974
set firewall system-output disable . . . 975
set firewall time-range periodic start . . . 976
set firewall time-range periodic end . . . 977
run show filter . . . 978
run show timerange . . . 979
QoS Configuration Commands . . . 980
class-of-service classifier <classifier-name> . . . 982
class-of-service classifier <classifier-name> forwarding-class <forwarding-class-name> code-point <code-point> . . . 983
class-of-service classifier <classifier-name> trust-mode <trust-mode> . . . 984
class-of-service forwarding-class <forwarding-class-name> local-priority <local-priority> . . . 985
class-of-service interface <port> classifier <classifier-name> . . . 986
class-of-service scheduler <scheduler-name> guaranteed-rate <guaranteed-rate> . . . 987
class-of-service scheduler <scheduler-name> mode SP . . . 988
class-of-service scheduler <scheduler-name> mode WFQ . . . 989
class-of-service scheduler <scheduler-name> mode WRR . . . 990
class-of-service scheduler <scheduler-name> weight <weight-id> . . . 991
class-of-service scheduler-profile <scheduler-profile-name> forwarding-class <forwarding-class-name> schedule <schedule-name> . . . 992
show class-of-service <text> . . . 993
set class-of-service interface scheduler-profile . . . 994
class-of-service interface <port> default-priority <default-priority-type> <default-priority-int> . . . 995
class-of-service pfc-profile <profile-name> code-point <code-point> drop <boolean> . . . 997
class-of-service interface <port> pfc-profile <profile-name> . . . 999
set firewall filter sequence then dscp . . . 1000
set class-of-service scheduler max-rate . . . 1001
CoPP Commands . . . 1002
set class-of-service forwarding-class local-priority . . . 1003
set class-of-service scheduler max-bandwidth-pps . . . 1004
set class-of-service scheduler min-bandwidth-pps . . . 1005
set class-of-service scheduler-profile copp-profile forwarding-classs scheduler . . . 1006
set class-of-service scheduler weight . . . 1007
set firewall filter copp sequence from destination-address-ipv4 . . . 1008
set firewall filter copp sequence from destination-address-ipv6 . . . 1009
set firewall filter copp sequence from destination-mac-address . . . 1010
set firewall filter copp sequence from destination-port . . . 1011
set firewall filter copp sequence from ether-type . . . 1012
set firewall filter copp sequence from protocol . . . 1013
set firewall filter copp sequence from source-address-ipv4 . . . 1014
set firewall filter copp sequence from source-address-ipv6 . . . 1015
set firewall filter copp sequence from source-mac-address . . . 1016

set firewall filter copp sequence from source-port 1017
set firewall filter copp sequence from vlan 1018

set firewall filter copp sequence then forwarding-class . . . 1019
set firewall filter copp sequence then dscp . . . 1020
run show copp bandwidth . . . 1021
run show copp statistics . . . 1022
run show filter copp . . . 1023
run show interface stm . . . 1024
run clear copp statistics . . . 1025
Buffer Management Commands . . . 1026
set interface ethernet-switching-options buffer egress-queue shared-ratio . . . 1027
set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared . . . 1028
run show gigabit-ethernet egress-queues . . . 1029
run show interface egress-buffer . . . 1030
Interface-based Rate Limiting Commands . . . 1031
set interface gigabit-ethernet rate-limiting ingress kilobits . . . 1032
set interface gigabit-ethernet rate-limiting ingress ratio . . . 1033
set interface gigabit-ethernet rate-limiting ingress burst . . . 1034
set interface gigabit-ethernet rate-limiting egress kilobits . . . 1035
set interface gigabit-ethernet rate-limiting egress ratio . . . 1036
set interface gigabit-ethernet rate-limiting egress burst . . . 1037
ACL-based Traffic Policer Commands . . . 1038
set firewall policer if-exceeding count-mode . . . 1039
set firewall policer if-exceeding rate-limit . . . 1040
set firewall policer if-exceeding burst-limit . . . 1041
set firewall filter sequence then policer . . . 1042
set firewall policer if-exceeding action discard . . . 1043
run show policer . . . 1044
PFC Watchdog . . . 1045
set class-of-service pfc-watchdog granularity . . . 1046
set class-of-service pfc-watchdog restore-action . . . 1047
set class-of-service pfc-watchdog code-point detect-interval . . . 1048
set class-of-service pfc-watchdog code-point restore-interval . . . 1050
set class-of-service interface pfc-watchdog code-point enable . . . 1052
run show pfc-watchdog config . . . 1053
run show pfc-watchdog stats . . . 1054
Protocol Configuration Commands . . . 1055
protocols arp aging-time . . . 1057
set protocols arp interface address mac-address . . . 1058
set protocols arp interface proxy . . . 1059
set protocols arp inspection vlan disable . . . 1060
set protocols arp inspection access-list ip mac-address . . . 1061
set protocols arp inspection vlan access-list . . . 1062
set protocols arp inspection trust-port . . . 1063
run show arp . . . 1064
run show arp inspection dhcp-binding . . . 1065
run show arp inspection interface . . . 1066

run show arp inspection vlan . . . 1067
run show arp inspection access-list . . . 1068
run show arp inspection statistics vlan . . . 1069
protocols lacp interface <interface> priority . . . 1070
protocols lacp priority . . . 1071
protocols sflow agent-id . . . 1072
protocols sflow collector udp-port . . . 1073
protocols sflow disable . . . 1074
protocols sflow header-len . . . 1075
protocols sflow interface <port> disable . . . 1076
protocols sflow interface <port> header-len . . . 1077
protocols sflow interface <port> polling-interval . . . 1078
protocols sflow interface <port> sampling-rate egress . . . 1079
protocols sflow interface <port> sampling-rate ingress . . . 1080
protocols sflow polling-interval . . . 1081
protocols sflow sampling-rate egress . . . 1082
protocols sflow sampling-rate ingress . . . 1083
protocols sflow source-address . . . 1084
set protocols dhcp snooping vlan . . . 1085
set protocols dhcp snooping trust-port . . . 1086
set protocols dhcp snooping vlan option82-policy . . . 1087
set protocols dhcp snooping option82 circuit-id . . . 1089
set protocols dhcp snooping option82 remote-id . . . 1090
set protocols dhcp snooping option82 trust-all . . . 1091
set protocols dhcp snooping binding file . . . 1092
set protocols dhcp snooping binding write-delay . . . 1093
run show dhcp snooping binding . . . 1094
set protocols dhcp relay interface disable . . . 1095
set protocols dhcp relay interface dhcp-server-address . . . 1096
set protocols dhcp relay interface relay-agent-address . . . 1097
set protocols dhcp relay interface option82-policy . . . 1098
set protocols dhcp relay option82 circuit-id . . . 1100
set protocols dhcp relay option82 remote-id . . . 1101
set protocols dhcp relay option82 trust-all . . . 1102
set protocols dhcp server pool network . . . 1103
set protocols dhcp server pool range low . . . 1104
set protocols dhcp server pool range high . . . 1105
set protocols dhcp server pool domain-name . . . 1106
set protocols dhcp server pool dns-server . . . 1107
set protocols dhcp server pool default-router . . . 1108
set protocols dhcp server pool lease-time . . . 1109
set protocols dhcp server pool vrf . . . 1110
run show dhcp server binding address . . . 1111
run show dhcp server binding interface . . . 1112
set protocols dhcp6 relay interface disable . . . 1113

set protocols dhcp6 relay interface destination . . . 1114
set protocols dhcp6 relay interface remote-id . . . 1115
run show dhcp6 relay-stats . . . 1116
set protocols lacp interface rate . . . 1117
run show lldp neighbor . . . 1118
set protocols dhcp6 snooping vlan . . . 1119
set protocols dhcp6 snooping trust-port . . . 1120
set protocols dhcp6 snooping binding file . . . 1121
set protocols dhcp6 snooping binding write-delay . . . 1122
set protocols dhcp6 snooping vlan option-policy . . . 1123
set protocols dhcp6 snooping option37 remote-id . . . 1124
set protocols dhcp6 snooping option18 interface-id . . . 1125
set protocols dhcp6 snooping interface max-clients . . . 1126
run show dhcp6 snooping binding . . . 1127
set protocols dhcp6 guard policy device-role . . . 1128
set protocols dhcp6 guard policy trust-port . . . 1129
set protocols dhcp6 guard policy interface . . . 1130
set protocols dhcp6 guard policy preference-min . . . 1131
set protocols dhcp6 guard policy preference-max . . . 1132
set protocols dhcp6 guard policy match server source-address . . . 1133
set protocols dhcp6 guard policy match reply ia-prefix . . . 1134
run show dhcp6 guard policy . . . 1135
run show dhcp6 guard . . . 1136
IP Multicast Commands . . . 1137
IGMP Snooping Configuration Commands . . . 1139
run show igmp-snooping . . . 1140
run show igmp-snooping groups . . . 1141
run show igmp-snooping mrouter . . . 1142
run show igmp-snooping querier . . . 1143
set protocols igmp-snooping enable . . . 1144
set protocols igmp-snooping interface max-groups . . . 1145
set protocols igmp-snooping last-member-query-count . . . 1146
set protocols igmp-snooping last-member-query-interval . . . 1147
set protocols igmp-snooping max-response-time . . . 1148
set protocols igmp-snooping query-interval . . . 1149
set protocols igmp-snooping report-suppression . . . 1150
set protocols igmp-snooping robustness-variable . . . 1151
set protocols igmp-snooping vlan-id enable . . . 1152
set protocols igmp-snooping vlan-id fast-leave . . . 1153
set protocols igmp-snooping vlan-id mrouter interface . . . 1154
set protocols igmp-snooping vlan-id querier address . . . 1155
set protocols igmp-snooping vlan-id querier enable . . . 1156
set protocols igmp-snooping vlan-id querier other-querier-timer . . . 1157
set protocols igmp-snooping vlan-id querier version . . . 1158
set protocols igmp-snooping vlan-id static group interface . . . 1159

set protocols igmp-snooping vlan-id unregistered flood-all . . . 1160
IGMP Commands . . . 1161
set protocols igmp interface . . . 1162
set protocols igmp interface join-group . . . 1163
set protocols igmp interface query-interval . . . 1164
set protocols igmp interface query-max-response-time . . . 1165
set protocols igmp interface version . . . 1166
run show igmp groups . . . 1167
run show igmp interface . . . 1168
PIM Configuration Commands . . . 1170
set protocols pim ecmp . . . 1171
set protocols pim interface active-active . . . 1172
set protocols pim interface drpriority . . . 1173
set protocols pim interface hello holdtime . . . 1174
set protocols pim interface hello interval . . . 1175
set protocols pim interface sm . . . 1176
set protocols pim interface use-source . . . 1177
set protocols pim join-prune-interval . . . 1178
set protocols pim keep-alive-timer . . . 1179
set protocols pim packets . . . 1180
set protocols pim register-suppress-time . . . 1181
set protocols pim rp . . . 1182
set protocols pim spt-switchover infinity-and-beyond . . . 1183
set protocols pim ssm prefix-list . . . 1184
run show pim interface . . . 1185
run show pim rp-info . . . 1186
run show pim neighbor . . . 1187
run show pim upstream . . . 1188
run show mroute . . . 1189
mtrace . . . 1190
run show pim group-type . . . 1191
Multicast Source Discovery Protocol (MSDP) Commands . . . 1192
set protocols msdp mesh-group source . . . 1193
set protocols msdp mesh-group member . . . 1194
run show msdp mesh-group . . . 1195
run show msdp peer . . . 1196
run show msdp sa . . . 1198
Multicast VLAN Registration (MVR) Commands . . . 1200
run show igmp-snooping mvr mvlan . . . 1201
run show igmp-snooping mvr receiver-vlan . . . 1202
set protocols igmp-snooping vlan-id mvr receiver vlan-list . . . 1203
set protocols igmp-snooping vlan-id mvr source group . . . 1204
OpenFlow Commands in CrossFlow Mode . . . 1205
VXLAN Commands . . . 1206
vxlans source-interface address . . . 1207

vxlans udp-port . . . 1208
set vxlans vni <text> decapsulation mode . . . 1209
vxlans vni <text> encapsulation mode . . . 1210
vxlans vni <text> encapsulation vlan . . . 1211
vxlans vni <text> flood vtep . . . 1212
vxlans vni <text> flood vtep <ipv4-addr> mac-address . . . 1213
vxlans vni <text> flood vtep <ipv4-addr> traffic-type . . . 1214
set vxlans vni vlan . . . 1215
set vxlans tunnel-mac-leaning disable . . . 1216
OVSDB VTEP command . . . 1217
set protocols ovsdb controller <controller-name> address . . . 1218
set protocols ovsdb controller <controller-name> inactivity-probe-duration 30000 . . . 1219
set protocols ovsdb controller <controller-name> maximum-backoff-duration . . . 1220
set protocols ovsdb controller <controller-name> port . . . 1221
set protocols ovsdb controller c1 protocol . . . 1222
set protocols ovsdb interface . . . 1223
set protocols ovsdb management-ip . . . 1224
set protocols ovsdb ssl bootstrap . . . 1225
set protocols ovsdb ssl ca-cert . . . 1226
set protocols ovsdb ssl certificate . . . 1227
set protocols ovsdb ssl private-key . . . 1228
set vxlans ovsdb-managed . . . 1229
set protocols ovsdb controller vrf mgmt-vrf . . . 1230
set vxlans l3-vni prefix-routes-only . . . 1231
set vxlans l3-vni . . . 1232
set vxlans vni mcast-group . . . 1233
run show vxlan statistics . . . 1234
run clear vxlan statistics . . . 1235
run show vxlan vni . . . 1236
run show vxlan address-table . . . 1237
BGP EVPN Commands . . . 1238
run show bgp evpn route . . . 1239
run show bgp evpn summary . . . 1240
run show bgp evpn vni . . . 1241
run show evpn es . . . 1242
run show evpn mac vni . . . 1243
set interface aggregate-ethernet evpn mh es-df-pref . . . 1244
set interface aggregate-ethernet evpn mh es-id . . . 1245
set interface aggregate-ethernet evpn mh es-sys-mac . . . 1246
set l3-interface routed-interface router-mac . . . 1247
set l3-interface vlan-interface anycast address . . . 1248
set l3-interface vlan-interface anycast mac . . . 1249
set l3-interface vlan-interface router-mac . . . 1250
set protocols bgp evpn advertise-all-vni . . . 1251
set protocols bgp evpn advertise-default-gw . . . 1252

set protocols bgp evpn advertise ipv4-unicast . . . 1253
set protocols bgp evpn advertise ipv6-unicast . . . 1254
set protocols bgp evpn advertise-svi-ip . . . 1255
set protocols bgp evpn default-originate . . . 1256
set protocols bgp evpn disable-ead-evi-rx . . . 1257
set protocols bgp evpn disable-ead-evi-tx . . . 1258
set protocols bgp evpn vni . . . 1259
set protocols bgp evpn vni advertise-default-gw . . . 1260
set protocols bgp evpn vni advertise-subnet . . . 1261
set protocols bgp evpn vni advertise-svi-ip . . . 1262
set protocols bgp evpn vni rd . . . 1263
set protocols bgp evpn vni route-target type . . . 1264
set protocols bgp neighbor evpn activate . . . 1265
set protocols bgp neighbor evpn allowas-in . . . 1266
set protocols bgp neighbor evpn route-map . . . 1267
set protocols bgp neighbor evpn route-reflector-client . . . 1268
set protocols bgp vrf evpn advertise-pip ip . . . 1269
set protocols evpn mh mac-holdtime . . . 1270
set protocols evpn mh neigh-holdtime . . . 1271
set protocols evpn mh redirect-off . . . 1272
set protocols evpn mh startup-delay . . . 1273
set vxlans vni arp-nd-suppress disable . . . 1274
PoE Configuration Commands . . . 1275
set poe interface max-power . . . 1276
set poe interface detection-type . . . 1278
set poe interface enable . . . 1279
set poe interface mode . . . 1280
set poe interface priority . . . 1281
set poe interface threshold-mode . . . 1282
set poe power management-mode . . . 1283
set poe power mode . . . 1284
set poe interface lldp-negotiation . . . 1286
set poe power voltage . . . 1287
set protocols poe traceoptions flag all disable . . . 1288
run show poe interface . . . 1289
run show poe power . . . 1291
VRRP Commands . . . 1292
set protocols vrrp interface vrid . . . 1293
set protocols vrrp interface vrid disable . . . 1294
set protocols vrrp interface vrid version . . . 1295
set protocols vrrp interface vrid ip . . . 1296
set protocols vrrp interface vrid priority . . . 1297
set protocols vrrp interface vrid interval . . . 1298
set protocols vrrp interface vrid preempt enable . . . 1299
set protocols vrrp interface vrid load-balance disable . . . 1300

set protocols vrrp interface vrid load-balance virtual-mac time-interval . . . 1301
set protocols vrrp interface vrid accept disable . . . 1302
set protocols vrrp interface vrid authentication type . . . 1303
set protocols vrrp interface vrid simple-key . . . 1304
set protocols vrrp interface vrid md5-key . . . 1305
run show vrrp . . . 1306
set protocols vrrp interface vrid ipv6-nd adv-interval-option . . . 1307
set protocols vrrp interface vrid ipv6-nd home-agent-config-flag . . . 1308
set protocols vrrp interface vrid ipv6-nd home-agent-lifetime . . . 1309
set protocols vrrp interface vrid ipv6-nd home-agent-preference . . . 1310
set protocols vrrp interface vrid ipv6-nd managed-config-flag . . . 1311
set protocols vrrp interface vrid ipv6-nd mtu . . . 1312
set protocols vrrp interface vrid ipv6-nd other-config-flag . . . 1313
set protocols vrrp interface vrid ipv6-nd prefix off-link . . . 1314
set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime . . . 1315
set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime . . . 1316
set protocols vrrp interface vrid ipv6-nd prefix router-address . . . 1317
set protocols vrrp interface vrid ipv6-nd ra-fast-retrans . . . 1318
set protocols vrrp interface vrid ipv6-nd ra-interval . . . 1319
set protocols vrrp interface vrid ipv6-nd ra-lifetime . . . 1320
set protocols vrrp interface vrid ipv6-nd reachable-time . . . 1321
set protocols vrrp interface vrid ipv6-nd router-preference . . . 1322
set protocols vrrp interface vrid ipv6-nd suppress-ra . . . 1323
Spanning Tree Protocol Commands . . . 1324
run show spanning-tree . . . 1326
run show spanning-tree mstp . . . 1327
run show spanning-tree pvst . . . 1329
run show spanning-tree rstp . . . 1330
run show spanning-tree statistics . . . 1331
run show spanning-tree stp . . . 1332
set protocols spanning-tree enable . . . 1333
set protocols spanning-tree force-version . . . 1334
set protocols spanning-tree interface enable . . . 1335
set protocols spanning-tree mstp bridge-priority . . . 1336
set protocols spanning-tree mstp configuration-name . . . 1337
set protocols spanning-tree mstp forward-delay . . . 1338
set protocols spanning-tree mstp hello-time . . . 1339
set protocols spanning-tree mstp interface bpdu-filter . . . 1340
set protocols spanning-tree mstp interface bpdu-guard . . . 1341
set protocols spanning-tree mstp interface edge . . . 1342
set protocols spanning-tree mstp interface external-path-cost . . . 1343
set protocols spanning-tree mstp interface internal-path-cost . . . 1344
set protocols spanning-tree mstp interface manual-forwarding . . . 1345
set protocols spanning-tree mstp interface mode . . . 1346
set protocols spanning-tree mstp interface port-priority . . . 1347

set protocols spanning-tree mstp interface root-guard . . . 1348
set protocols spanning-tree mstp interface tcn-guard . . . 1349
set protocols spanning-tree mstp max-age . . . 1350
set protocols spanning-tree mstp max-hops . . . 1351
set protocols spanning-tree mstp msti bridge-priority . . . 1352
set protocols spanning-tree mstp msti interface cost . . . 1353
set protocols spanning-tree mstp msti interface port-priority . . . 1354
set protocols spanning-tree mstp msti vlan . . . 1355
set protocols spanning-tree mstp revision-level . . . 1356
set protocols spanning-tree pvst interface bpdu-guard . . . 1357
set protocols spanning-tree pvst interface manual-forwarding . . . 1358
set protocols spanning-tree pvst interface mode . . . 1359
set protocols spanning-tree pvst interface root-guard . . . 1360
set protocols spanning-tree pvst vlan bridge-priority . . . 1361
set protocols spanning-tree pvst vlan enable . . . 1362
set protocols spanning-tree pvst vlan forward-delay . . . 1363
set protocols spanning-tree pvst vlan hello-time . . . 1364
set protocols spanning-tree pvst vlan interface path-cost . . . 1365
set protocols spanning-tree pvst vlan interface port-priority . . . 1366
set protocols spanning-tree pvst vlan max-age . . . 1367
set protocols spanning-tree rstp bridge-priority . . . 1368
set protocols spanning-tree rstp forward-delay . . . 1369
set protocols spanning-tree rstp hello-time . . . 1370
set protocols spanning-tree rstp interface bpdu-filter . . . 1371
set protocols spanning-tree rstp interface bpdu-guard . . . 1372
set protocols spanning-tree rstp interface edge . . . 1373
set protocols spanning-tree rstp interface mode . . . 1374
set protocols spanning-tree rstp interface path-cost . . . 1375
set protocols spanning-tree rstp interface port-priority . . . 1376
set protocols spanning-tree rstp interface root-guard . . . 1377
set protocols spanning-tree rstp interface tcn-guard . . . 1378
set protocols spanning-tree rstp max-age . . . 1379
set protocols spanning-tree stp bridge-priority . . . 1380
set protocols spanning-tree stp forward-delay . . . 1381
set protocols spanning-tree stp hello-time . . . 1382
set protocols spanning-tree stp interface bpdu-filter . . . 1383
set protocols spanning-tree stp interface bpdu-guard . . . 1384
set protocols spanning-tree stp interface edge . . . 1385
set protocols spanning-tree stp interface mode . . . 1386
set protocols spanning-tree stp interface path-cost . . . 1387
set protocols spanning-tree stp interface port-priority . . . 1388
set protocols spanning-tree stp interface root-guard . . . 1389
set protocols spanning-tree stp interface tcn-guard . . . 1390
set protocols spanning-tree stp max-age . . . 1391
MLAG Commands . . . 1392

set protocols mlag domain . . . 1393
set protocols mlag domain node . . . 1394
set protocols mlag domain interface link . . . 1395
set protocols mlag domain peer-ip peer-link . . . 1396
set protocols mlag domain peer-ip peer-vlan . . . 1397
run show mlag domain . . . 1398
run show mlag link . . . 1399
run show mlag consistency-parameter . . . 1400
GRE Tunnel Interface Commands . . . 1402
run show l3-interface tunnel . . . 1403
set l3-interface tunnel address . . . 1404
set l3-interface tunnel destination . . . 1405
set l3-interface tunnel disable . . . 1406
set l3-interface tunnel source . . . 1407
set l3-interface tunnel tunnel-mode gre-ip . . . 1408
set l3-interface tunnel vrf . . . 1409
GVRP Commands . . . 1410
set protocols gvrp join-timer . . . 1411
set protocols gvrp leave-timer . . . 1412
set protocols gvrp leaveall-timer . . . 1413
run clear gvrp interface statistics . . . 1414
run show gvrp interface . . . 1415
run show gvrp interface statistics . . . 1416
set protocols gvrp edge-switch . . . 1417
set protocols gvrp enable . . . 1418
set protocols gvrp interface enable . . . 1419
set protocols gvrp traceoptions flag config . . . 1420
set protocols gvrp traceoptions flag packets . . . 1421
MVRP Commands . . . 1422
run clear mvrp interface statistics . . . 1423
run show mvrp interface . . . 1424
run show mvrp interface statistics . . . 1425
set protocols mvrp edge-switch . . . 1426
set protocols mvrp enable . . . 1427
set protocols mvrp interface enable . . . 1428
set protocols mvrp traceoptions flag config . . . 1429
set protocols mvrp traceoptions flag packets . . . 1430
set protocols mvrp join-timer . . . 1431
set protocols mvrp leave-timer . . . 1432
set protocols mvrp leaveall-timer . . . 1433
ERPS Commands . . . 1434
run show erps brief . . . 1435
run show erps interface . . . 1436
run show erps ring . . . 1437
run show erps statistics . . . 1439

set protocols erps enable . . . 1440
set protocols erps ring . . . 1441
set protocols erps version . . . 1442
set protocols erps ring instance . . . 1443
set protocols erps ring instance control-vlan . . . 1444
set protocols erps ring instance description . . . 1445
set protocols erps ring instance enable . . . 1446
set protocols erps ring instance guard-timer . . . 1447
set protocols erps ring instance holdoff-timer . . . 1448
set protocols erps ring instance protected-instance . . . 1449
set protocols erps ring instance r-aps level . . . 1450
set protocols erps ring instance rpl . . . 1451
set protocols erps ring instance wtr-timer . . . 1452
set protocols erps ring port0 interface . . . 1453
set protocols erps ring port1 interface . . . 1454
set protocols erps ring r-aps ring-mac . . . 1455
set protocols erps ring sub-ring . . . 1456
set protocols erps ring virtual-channel . . . 1457
set protocols erps ring instance non-revertive . . . 1458
set protocols erps tcn-propagation . . . 1459
set protocols erps ring instance connect ring . . . 1460
erps switch force ring instance . . . 1461
erps switch manual ring instance . . . 1462
erps clear ring ring instance . . . 1463
set protocols erps traceoptions flag all disable . . . 1464
set protocols erps traceoptions flag config disable . . . 1465
set protocols erps traceoptions flag ring disable . . . 1466
EFM OAM Commands . . . 1467
set protocols ethernet-oam interface enable . . . 1468
set protocols ethernet-oam interface mode . . . 1469
set protocols ethernet-oam interface remote-loopback supported . . . 1470
set protocols ethernet-oam interface remote-loopback timeout . . . 1471
ethernet-oam remote-loopback start|stop interface . . . 1472
set protocols ethernet-oam interface timeout . . . 1474
set protocols ethernet-oam traceoptions flag packets . . . 1475
set protocols ethernet-oam traceoptions flag config . . . 1476
run show ethernet-oam . . . 1477
run show ethernet-oam statistics . . . 1479
Loopback Detection Commands . . . 1480
set protocols loopback-detection enable . . . 1481
set protocols loopback-detection interface enable . . . 1482
set protocols loopback-detection message-interval . . . 1483
set protocols loopback-detection traceoptions configuration disable . . . 1484
set protocols loopback-detection traceoptions all disable . . . 1485
run show loopback-detection . . . 1486

run clear loopback-detection interface 1487

PICOS Routing and Switching Command Reference

Command-Line Interface Commands

- copy running-config startup-config
- set cli idle-timeout
- set cli screen-length
- set cli terminal
- syslog monitor
- syslog notify
- hwclock
- rollback

System Management Commands

- NAC Configuration Commands
  - set protocols dot1x aaa radius authentication server-ip
  - set protocols dot1x aaa radius authentication server-ip priority
  - set protocols dot1x aaa radius authentication server-ip retry-num
  - set protocols dot1x aaa radius authentication server-ip retry-interval
  - set protocols dot1x aaa radius authentication server-ip detect-interval
  - set protocols dot1x interface auth-mode 802.1x
  - set protocols dot1x interface auth-mode 802.1x fallback-to-web disable
  - set protocols dot1x interface auth-mode mac-radius
  - set protocols dot1x interface auth-mode web
  - set protocols dot1x interface authentication-open disable
  - set protocols dot1x aaa radius dynamic-author client
  - set protocols dot1x aaa radius dynamic-author client shared-key
  - set protocols dot1x aaa radius nas-ip
  - set protocols dot1x aaa radius accounting disable
  - set protocols dot1x interface host-mode
  - set protocols dot1x block-vlan-id
  - set protocols dot1x server-fail-vlan-id
  - set protocols dot1x filter sequence from destination-address-ipv4
  - set protocols dot1x filter sequence from destination-address-ipv6
  - set protocols dot1x filter sequence from destination-port
  - set protocols dot1x filter sequence from ether-type
  - set protocols dot1x filter sequence from source-address-ipv4
  - set protocols dot1x filter sequence from source-address-ipv6
  - set protocols dot1x filter sequence from source-port
  - set protocols dot1x filter sequence from protocol
  - set protocols dot1x filter sequence then action
  - run show dot1x all
  - run show dot1x interface
  - run show dot1x server
  - run show dot1x dynamic filter
  - run show dot1x downloadable filter
  - run show dot1x interface statistics gigabit-ethernet
  - set protocols dot1x server-fail recovery-method
  - set protocols dot1x aaa radius authentication server-ip consecutive-detect-num
  - set protocols dot1x aaa vrf mgmt-vrf
  - set protocols dot1x interface session-timeout
  - set protocols dot1x interface recovery-timeout
  - set protocols dot1x server-fail recovery-timeout
  - set protocols dot1x interface max-sessions
  - set protocols dot1x max-sessions-per-port
  - set protocols dot1x aaa radius authentication server-ip auth-port
  - set protocols dot1x aaa radius authentication server-ip acct-port
  - set protocols dot1x aaa radius dynamic-author client port
  - run show dot1x radius-port
  - set protocols dot1x filter sequence from destination-mac-address
  - set protocols dot1x filter sequence from vlan
- SNMP Configuration Commands
  - set protocols snmp trap-group targets security-name

- set protocols lldp snmp-trap
- set protocols snmp trap-group event cpu-threshold enable
- set protocols snmp trap-group event cpu-threshold high
- set protocols snmp trap-group event cpu-threshold interval
- set protocols snmp trap-group event cpu-threshold low
- set protocols snmp trap-group event mac-threshold enable
- set protocols snmp trap-group event mac-threshold interval
- set protocols snmp trap-group event mac-threshold limit
- set protocols snmp trap-group vrf mgmt-vrf
- set protocols snmp trap-group version
- set protocols snmp v3 enable
- set protocols snmp v3 usm-user
- set protocols snmp v3 usm-user group
- set protocols snmp v3 group notify-view
- set protocols snmp v3 group read-view
- set protocols snmp v3 group write-view
- set protocols snmp v3 group security-level
- set protocols snmp v3 usm-user authentication-mode
- set protocols snmp v3 usm-user authentication-key
- set protocols snmp v3 usm-user privacy-mode
- set protocols snmp v3 usm-user privacy-key
- set protocols snmp v3 mib-view subtree mask
- set protocols snmp v3 mib-view subtree type
- set protocols snmp trap-group source-interface
- set protocols snmp community
- set protocols snmp community authorization
- set protocols snmp community clients
- set protocols snmp contact
- set protocols snmp location
- run show snmp statistics

- Mirror Configuration Commands
  - set interface ethernet-switching-options analyzer input
  - set interface ethernet-switching-options analyzer output
  - set interface ethernet-switching-options analyzer erspan input
  - set interface ethernet-switching-options analyzer erspan output source-ip
  - set interface ethernet-switching-options analyzer erspan output dest-ip
  - set interface ethernet-switching-options analyzer erspan output vrf
  - run show analyzer
  - set firewall filter sequence then erspan source-ip
  - set firewall filter sequence then erspan dest-ip
  - set firewall filter sequence then erspan vrf
  - set firewall filter sequence then erspan ttl
- RMON Commands
  - run show rmon alarms
  - run show rmon eventlog
  - run show rmon events
  - run show rmon history
  - run show rmon statistics
  - set protocols snmp rmon alarm falling-event-index
  - set protocols snmp rmon alarm falling-threshold
  - set protocols snmp rmon alarm interval
  - set protocols snmp rmon alarm owner
  - set protocols snmp rmon alarm rising-event-index
  - set protocols snmp rmon alarm rising-threshold
  - set protocols snmp rmon alarm sample-type
  - set protocols snmp rmon alarm variable
  - set protocols snmp rmon event community
  - set protocols snmp rmon event description
  - set protocols snmp rmon event owner
  - set protocols snmp rmon event type
  - set protocols snmp rmon history buckets
  - set protocols snmp rmon history interface
  - set protocols snmp rmon history interval
  - set protocols snmp rmon history owner
  - set protocols snmp rmon statistics interface
  - set protocols snmp rmon statistics owner
- RESTCONF Commands
  - set protocols restconf
  - set protocols restconf port
  - set protocols restconf traceoptions flag config disable
  - set protocols restconf traceoptions flag all disable

    - set protocols restconf traceoptions flag datastore disable
- run show system boot-messages
- run show system connections
- run show system core-dumps
- run show system cpu-usage
- run show system date
- run show system fan
- run show system memory-usage
- run show system name
- run show system ntp-status
- run show system os
- run show system processes brief
- run show system processes detail
- run show system rollback compare to
- run show system rollback file
- run show system rollback list
- run show system rpsu
- run show system serial-number
- run show system temperature
- run show system uptime
- run show system users
- set system aaa local disable
- set system aaa radius accounting disable
- set system aaa radius accounting server-ip
- set system aaa radius accounting server-ip port
- set system aaa radius accounting server-ip shared-key
- set system aaa radius accounting server-ip timeout
- set system aaa radius authorization disable
- set system aaa radius authorization server-ip
- set system aaa radius authorization server-ip port
- set system aaa radius authorization server-ip shared-key
- set system aaa radius authorization server-ip timeout
- set system aaa radius vrf mgmt-vrf
- set system aaa tacacs-plus accounting
- set system aaa tacacs-plus authorization
- set system aaa tacacs-plus auth-type
- set system aaa tacacs-plus disable
- set system aaa tacacs-plus key
- set system aaa tacacs-plus port-number
- set system aaa tacacs-plus timeout
- set system aaa tacacs-plus server-ip
- set system aaa tacacs-plus source-interface
- set system aaa local-auth-fallback disable
- set system aaa tacacs-plus vrf mgmt-vrf
- set system hostname
- set system inband vlan-interface
- set system inband loopback
- set system inband routed-interface
- set system inband enable
- system login-acl network
- system login announcement
- system login user
- system login user admin class
- set system login user authentication plain-text-password
- system login user class
- set system timezone
- set system ntp server-ip
- set system ntp source-interface
- set system ntp vrf mgmt-vrf
- set interface gigabit-ethernet ptp mode
- set system services ssh connection-limit
- set system services ssh disable
- set system services ssh protocol-version v2
- set system services ssh rate-limit
- set system services ssh root-login
- set system services ssh idle-timeout
- set system services ssh port
- set system snmp-acl security-name network
- set system syslog server-ip
- set system syslog local-file
- set system syslog vrf mgmt-vrf

- set system usb disable
- set system management-ethernet eth0 ip-address {IPv4 | IPv6}
- set system management-ethernet eth0 ip-gateway {IPv4 | IPv6}
- show system management-ethernet
- run request system reboot
- run show system hwinfo
- ping
- traceroute
- tftp
- set protocols sflow collector vrf mgmt-vrf
- scp
- set system login banner
- upgrade2 image-file
- upgrade2 image-file backup-file
- upgrade2 image-file factory-default
- upgrade2 image-file use-prev-config
- set system dns-server-ip
- set system console idle-timeout
- set system login multiline-banner message
- set system login multiline-announcement message
- set system aaa radius source-interface
- set protocols grpc enable
- set protocols grpc port
- set system ztp enable
- telnet
- set system start-shell-sh password
- set system services telnet disable

Interface Configuration Commands

- Port Security Commands
  - set interface gigabit-ethernet port-security mac-address vlan
  - set interface gigabit-ethernet port-security mac-limit
  - set interface gigabit-ethernet port-security sticky
  - set interface gigabit-ethernet port-security violation
  - set interface gigabit-ethernet port-security block
  - set interface ethernet-switching-options port-error-discard timeout
  - run show port-security brief
  - run show port-security address
  - run show port-security interface
  - run clear port-security port-error
  - run clear port-security sticky interface
  - run clear port-security sticky address
  - run clear port-security dynamic interface
  - run clear port-security dynamic address
- L3 Interface
  - set l3-interface vlan-interface vrf
  - set l3-interface vlan-interface address prefix-length
  - set l3-interface loopback address
  - set l3-interface loopback disable
  - set l3-interface loopback vrf
  - set l3-interface vlan-interface rate-limit
  - set l3-interface vlan-interface mtu
  - set l3-interface vlan-interface dhcp
  - run show l3-interface vlan-interface
  - run show l3-interface
  - run show l3-interface loopback
  - run clear l3-interface statistics
  - set l3-interface routed-interface dhcp
  - set l3-interface routed-interface rate-limit
  - set l3-interface routed-interface mtu
  - set l3-interface routed-interface vrf
  - set l3-interface routed-interface address
  - set l3-interface routed-interface description
  - run show l3-interface routed-interface
  - set l3-interface vlan-interface pmtu-discovery
  - set l3-interface routed-interface pmtu-discovery
- Routed Interface
  - run show interface routed-interface brief
  - run show vlans routed-vlan
  - set interface aggregate-ethernet routed-interface enable
  - set interface aggregate-ethernet routed-interface name

    - set interface aggregate-ethernet routed-interface sub-interface vlan-id
    - set interface gigabit-ethernet routed-interface enable
    - set interface gigabit-ethernet routed-interface sub-interface
    - set vlans reserved-vlan
    - set interface gigabit-ethernet routed-interface name
- Uplink Failure Detection Commands
    - run show interface ufd
    - set interface ufd link-to-monitor
    - set interface ufd link-to-disable
- IPv6 Neighbor Discovery Protocol Command Reference
    - set l3-interface routed-interface ipv6-nd adv-interval-option
    - set l3-interface routed-interface ipv6-nd home-agent-config-flag
    - set l3-interface routed-interface ipv6-nd home-agent-lifetime
    - set l3-interface routed-interface ipv6-nd home-agent-preference
    - set l3-interface routed-interface ipv6-nd managed-config-flag
    - set l3-interface routed-interface ipv6-nd mtu
    - set l3-interface routed-interface ipv6-nd other-config-flag
    - set l3-interface routed-interface ipv6-nd prefix off-link
    - set l3-interface routed-interface ipv6-nd prefix preferred-lifetime
    - set l3-interface routed-interface ipv6-nd prefix router-address
    - set l3-interface routed-interface ipv6-nd prefix valid-lifetime
    - set l3-interface routed-interface ipv6-nd ra-fast-retrans
    - set l3-interface routed-interface ipv6-nd ra-interval
    - set l3-interface routed-interface ipv6-nd ra-lifetime
    - set l3-interface routed-interface ipv6-nd reachable-time
    - set l3-interface routed-interface ipv6-nd router-preference
    - set l3-interface routed-interface ipv6-nd suppress-ra
    - set l3-interface vlan-interface ipv6-nd adv-interval-option
    - set l3-interface vlan-interface ipv6-nd home-agent-config-flag
    - set l3-interface vlan-interface ipv6-nd home-agent-lifetime
    - set l3-interface vlan-interface ipv6-nd home-agent-preference
    - set l3-interface vlan-interface ipv6-nd managed-config-flag
    - set l3-interface vlan-interface ipv6-nd mtu
    - set l3-interface vlan-interface ipv6-nd other-config-flag
    - set l3-interface vlan-interface ipv6-nd prefix off-link
    - set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime
    - set l3-interface vlan-interface ipv6-nd prefix router-address
    - set l3-interface vlan-interface ipv6-nd prefix valid-lifetime
    - set l3-interface vlan-interface ipv6-nd ra-fast-retrans
    - set l3-interface vlan-interface ipv6-nd ra-interval
    - set l3-interface vlan-interface ipv6-nd ra-lifetime
    - set l3-interface vlan-interface ipv6-nd reachable-time
    - set l3-interface vlan-interface ipv6-nd router-preference
    - set l3-interface vlan-interface ipv6-nd suppress-ra
- set management-ethernet-speed eth0
- set interface gigabit-ethernet up-mode
- set interface gigabit-ethernet speed
- show interface bpdu-tunneling
- show interface aggregate-ethernet <lag_name>
- show interface aggregate-ethernet <lag_name> dot1q-tunneling
- show interface brief
- show interface detail
- show interface diagnostics optics all
- show interface ecmp max-path
- show interface flexlink
- show interface gigabit-ethernet <interface>
- set interface gigabit-ethernet fec
- set interface gigabit-ethernet family ethernet-switching vlan members
- set interface gigabit-ethernet family ethernet-switching port-mode
- set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol
- set interface gigabit-ethernet ether-options 802.3ad
- set interface gigabit-ethernet duplex auto
- set interface gigabit-ethernet cdr
- set interface gigabit-ethernet breakout
- set interface gigabit-ethernet auto-speeds
- set interface ecmp hash-mapping field vlan disable
- set interface ecmp hash-mapping field port-source disable
- set interface ecmp hash-mapping field port-destination disable
- set interface ecmp hash-mapping field ip-source disable
- set interface ecmp hash-mapping field ip-protocol disable
- set interface ecmp hash-mapping field ip-destination disable

- set interface ecmp hash-mapping field ingress-interface disable
- set interface bpdu-tunneling destination-mac
- set interface aggregate-ethernet family ethernet-switching vlan members
- set interface aggregate-ethernet family ethernet-switching port-mode
- set interface aggregate-ethernet disable
- set interface aggregate-ethernet description
- set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout
- set interface aggregate-ethernet aggregated-ether-options lacp fallback enable
- set interface aggregate-ethernet aggregated-ether-options lacp
- set interface aggregate-ethernet
- run show interface port-index-mapping
- run show interface diagnostics tdr
- interface max-route-limit
- interface max-acl-rule-limit <egress/ingress>
- interface gigabit-ethernet <port> wred queue <value> min_thresh
- interface gigabit-ethernet <port> wred queue <value> max_thresh
- interface gigabit-ethernet <port> wred queue <value> enable
- interface gigabit-ethernet <port> wred queue <value> ecn_thresh
- interface gigabit-ethernet <port> wred queue <value> drop_probability
- interface gigabit-ethernet <port> storm-control <mode> ratio <value>
- interface gigabit-ethernet <port> storm-control <mode> pps
- interface gigabit-ethernet <port> storm-control <mode> kbps
- interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id>
- interface gigabit-ethernet <port> snmp-trap
- interface gigabit-ethernet <port> power-preemphasis-level
- interface gigabit-ethernet <port> mtu
- interface gigabit-ethernet <port> mac-learning <boolean>
- interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>
- interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>
- interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged
- interface gigabit-ethernet <port> family ethernet-switching native-vlan-id
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress
- interface gigabit-ethernet <port> disable
- interface gigabit-ethernet <port> ether-options flow-control
- interface gigabit-ethernet <port> description
- interface gigabit-ethernet <port> crossflow local-control
- interface gigabit-ethernet <port> crossflow enable
- interface gigabit-ethernet <port> backup-port mode
- interface gigabit-ethernet <port> backup-port interface
- interface gigabit-ethernet <port> backup-port delay
- interface ethernet-switching-options mac-table-aging-time
- interface ethernet-switching-options buffer queue-limit
- interface ecmp max-path
- interface cut-through-mode
- interface aggregate-ethernet <lag_name> storm-control <mode> pps
- interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan
- interface aggregate-ethernet <lag_name> snmp-trap
- interface aggregate-ethernet <lag_name> mtu
- interface aggregate-ethernet <lag_name> hash-mapping mode
- interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress
- interface aggregate-ethernet <lag_name> crossflow local-control
- interface aggregate-ethernet <lag_name> crossflow enable
- interface aggregate-ethernet <lag_name> backup-port mode
- interface aggregate-ethernet <lag_name> backup-port interface
- interface aggregate-ethernet <lag_name> backup-port delay
- interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port
- interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control
- interface aggregate-balancing hash-mapping field vlan disable
- interface aggregate-balancing hash-mapping field port-source disable
- interface aggregate-balancing hash-mapping field port-destination disable
- interface aggregate-balancing hash-mapping field ip-source disable
- interface aggregate-balancing hash-mapping field ip-protocol disable
- interface aggregate-balancing hash-mapping field ip-destination disable
- interface aggregate-balancing hash-mapping field ingress-interface disable

- interface aggregate-balancing hash-mapping field ethernet-type disable
- interface aggregate-balancing hash-mapping field ethernet-source-address disable
- interface aggregate-balancing hash-mapping field ethernet-destination-address disable
- set interface ecmp hash-mapping randomized-load-balancing
- set interface ecmp hash-mapping round-robin-load-balancing
- set interface ecmp hash-mapping dlb-normal
- set interface ecmp hash-mapping symmetric

VLAN Configuration Commands

- set vlans dot1q-tunneling egress from
- set vlans dot1q-tunneling egress then action
- set vlans dot1q-tunneling egress then service-vlan
- set vlans dot1q-tunneling ingress from double-tag service-vlan
- set vlans dot1q-tunneling ingress from one-tag customer-vlan-list
- set vlans dot1q-tunneling ingress from untag enabled
- set vlans dot1q-tunneling ingress then
- set vlans vlan-id
- set vlans vlan-id description
- set vlans vlan-id l3-interface
- set vlans vlan-id vlan-name
- set vlans vlan-id private-vlan mode
- set vlans vlan-id private-vlan association
- set mac-map mac-address vlan
- run show vlans
- run show vlans private-vlan
- run show vlans private-vlan type
- run show mac-map
- set tracemac disable
- tracemac

Voice VLAN Configuration Commands

- set interface gigabit-ethernet voice-vlan mode
- set interface gigabit-ethernet voice-vlan tagged mode
- set interface gigabit-ethernet voice-vlan vlan-id
- set vlans voice-vlan aging
- set vlans voice-vlan dscp
- set vlans voice-vlan local-priority
- set vlans voice-vlan mac-address mask
- set vlans voice-vlan mac-address description
- show vlans voice-vlan
- show vlans voice-vlan oui
- show vlans voice-vlan vlan-id <text>

Layer 3 Routing Commands

- run show neighbors
- run show route
- run show route forward-host
- run show route forward-route
- run show vrf
- set ip vrf
- set ip routing enable
- set system management-vrf enable
- BGP Commands
  - run show bgp
  - run show bgp neighbor
  - run show bgp route
  - run show bgp unicast neighbor graceful-restart
  - set protocols bgp aggregate-address
  - set protocols bgp always-compare-med
  - set protocols bgp bestpath as-path type multipath-relax
  - set protocols bgp bestpath bandwidth
  - set protocols bgp bestpath compare-routerid
  - set protocols bgp bestpath med missing-as-worst
  - set protocols bgp cluster-id
  - set protocols bgp graceful-shutdown
  - set protocols bgp listen
  - set protocols bgp local-as
  - set protocols bgp max-med
  - set protocols bgp multipath maximum-paths

- set protocols bgp neighbor activate
- set protocols bgp neighbor addpath-tx-all-paths
- set protocols bgp neighbor addpath-tx-bestpath-per-as
- set protocols bgp neighbor advertisement-interval
- set protocols bgp neighbor allowas-in
- set protocols bgp neighbor as-override
- set protocols bgp neighbor capability extended-nexthop
- set protocols bgp neighbor default-originate
- set protocols bgp neighbor description
- set protocols bgp neighbor disable-connected-check
- set protocols bgp neighbor ebgp-multihop
- set protocols bgp neighbor filter-list
- set protocols bgp neighbor next-hop-self
- set protocols bgp neighbor password
- set protocols bgp neighbor peer-group
- set protocols bgp neighbor prefix-list
- set protocols bgp neighbor remote-as
- set protocols bgp neighbor remove-private-as
- set protocols bgp neighbor route-map
- set protocols bgp neighbor route-reflector-client
- set protocols bgp neighbor send-community
- set protocols bgp neighbor shutdown
- set protocols bgp neighbor soft-reconfiguration
- set protocols bgp neighbor timers connect
- set protocols bgp neighbor timers holdtime
- set protocols bgp neighbor timers keepalive
- set protocols bgp neighbor ttl-security hops
- set protocols bgp neighbor update-source
- set protocols bgp network
- set protocols bgp network-import-check
- set protocols bgp peer-group
- set protocols bgp redistribute
- set protocols bgp route-map delay-timer
- set protocols bgp router-id
- set protocols bgp table-map
- set protocols bgp timers
- set protocols bgp update-delay
- set protocols bgp ebgp-requires-policy
- set protocols bgp neighbor timers delayopen
- set protocols bgp neighbor maximum-prefix
- set protocols bgp neighbor maximum-prefix-out
- set protocols bgp neighbor port
- set protocols bgp neighbor sender-as-path-loop-detection
- set protocols bgp fast-external-failover
- set protocols bgp confederation identifier
- set protocols bgp confederation peers
- set protocols bgp dampening
- set protocols bgp default local-preference
- set protocols bgp as-notation
- set protocols bgp neighbor local-as

- OSPFv2 Commands
  - run clear ospf interface
  - run show ospf border-routers
  - run show ospf database
  - run show ospf interface
  - run show ospf neighbor
  - run show ospf route
  - run show ospf summary-address
  - set protocols ospf aggregation timer
  - set protocols ospf area area-type
  - set protocols ospf area filter-list prefix
  - set protocols ospf area no-summary
  - set protocols ospf area range
  - set protocols ospf area virtual-link
  - set protocols ospf area virtual-link authentication
  - set protocols ospf area virtual-link authentication-key
  - set protocols ospf area virtual-link dead-interval
  - set protocols ospf area virtual-link hello-interval
  - set protocols ospf area virtual-link message-digest-key md5
  - set protocols ospf area virtual-link retransmit-interval
  - set protocols ospf area virtual-link transmit-delay

    - set protocols ospf auto-cost reference-bandwidth
    - set protocols ospf compatible rfc1583
    - set protocols ospf default-information originate
    - set protocols ospf default-metric
    - set protocols ospf interface area
    - set protocols ospf interface authentication-key
    - set protocols ospf interface authentication message-digest
    - set protocols ospf interface cost
    - set protocols ospf interface dead-interval
    - set protocols ospf interface hello-interval
    - set protocols ospf interface message-digest-key md5
    - set protocols ospf interface network
    - set protocols ospf interface priority
    - set protocols ospf interface retransmit-interval
    - set protocols ospf interface transmit-delay
    - set protocols ospf log-adjacency-changes
    - set protocols ospf max-metric router-lsa administrative
    - set protocols ospf max-metric router-lsa on-shutdown
    - set protocols ospf max-metric router-lsa on-startup
    - set protocols ospf multi-instance disable
    - set protocols ospf network area
    - set protocols ospf passive-interface
    - set protocols ospf redistribute
    - set protocols ospf redistribute metric-type
    - set protocols ospf redistribute route-map
    - set protocols ospf router-id
    - set protocols ospf summary-address
    - set protocols ospf timers lsa min-arrival
    - set protocols ospf timers throttle spf
    - set protocols ospf traceoption ism
    - set protocols ospf traceoption lsa
    - set protocols ospf traceoption nsm
    - set protocols ospf traceoption packet
    - set protocols ospf traceoption zebra
    - set protocols ospf graceful-restart enable
    - set protocols ospf capability opaque
    - set protocols ospf graceful-restart grace-period
    - set protocols ospf graceful-restart helper enable
    - set protocols ospf graceful-restart helper planned-only
    - set protocols ospf graceful-restart helper strict-lsa-checking
    - set protocols ospf graceful-restart helper supported-grace-time
    - run graceful-restart prepare ospf
    - run show ospf graceful-restart helper
- OSPFv3 Command Reference
    - set protocols ospf6 area
    - set protocols ospf6 area range
    - set protocols ospf6 area stub
    - set protocols ospf6 area stub no-summary
    - set protocols ospf6 auto-cost reference-bandwidth
    - set protocols ospf6 distance
    - set protocols ospf6 distance-ospf6
    - set protocols ospf6 interface area
    - set protocols ospf6 interface cost
    - set protocols ospf6 interface dead-interval
    - set protocols ospf6 interface hello-interval
    - set protocols ospf6 interface ifmtu
    - set protocols ospf6 interface mtu-ignore
    - set protocols ospf6 interface network
    - set protocols ospf6 interface passive
    - set protocols ospf6 interface priority
    - set protocols ospf6 interface retransmit-interval
    - set protocols ospf6 interface transmit-delay
    - set protocols ospf6 log-adjacency-changes
    - set protocols ospf6 redistribute
    - set protocols ospf6 router-id
    - set protocols ospf6 stub-router administrative
    - set protocols ospf6 timers lsa min-arrival
    - set protocols ospf6 timers throttle spf
    - set protocols ospf6 traceoption
    - set protocols ospf6 traceoption border-routers
    - set protocols ospf6 traceoption lsa

    - set protocols ospf6 traceoption message
    - set protocols ospf6 traceoption neighbor
    - set protocols ospf6 traceoption route
    - set protocols ospf6 traceoption spf
    - set protocols ospf6 traceoption zebra
    - set protocols ospf6 graceful-restart enable
    - set protocols ospf6 capability opaque
    - set protocols ospf6 graceful-restart grace-period
    - set protocols ospf6 graceful-restart helper enable
    - set protocols ospf6 graceful-restart helper planned-only
    - set protocols ospf6 graceful-restart helper lsa-checking-disable
    - set protocols ospf6 graceful-restart helper supported-grace-time
    - run graceful-restart prepare ospf6
    - run show ospf6 graceful-restart helper
- Static Route Configuration Commands
    - set protocols static interface-route interface
    - set protocols static mroute
    - set protocols static route
- Route Map Commands
    - run show routing route-map
    - set routing as-path-list
    - set routing large-community-list expanded
    - set routing large-community-list standard
    - set routing prefix-list
    - set routing prefix-list description
    - set routing community-list expanded
    - set routing community-list standard
    - set routing extcommunity-list expanded
    - set routing extcommunity-list standard
    - set routing route-map set-action large-community
    - set routing route-map call
    - set routing route-map description
    - set routing route-map match as-path
    - set routing route-map match community
    - set routing route-map match community-with-exact-match
    - set routing route-map match evpn default-route
    - set routing route-map match evpn route-type
    - set routing route-map match evpn vni
    - set routing route-map match extcommunity
    - set routing route-map matching-policy
    - set routing route-map match interface
    - set routing route-map match ipv4-addr address
    - set routing route-map match ipv4-addr next-hop
    - set routing route-map match ipv4-addr route-source
    - set routing route-map match ipv6-addr
    - set routing route-map match large-community
    - set routing route-map match local-preference
    - set routing route-map match metric
    - set routing route-map match origin
    - set routing route-map match peer
    - set routing route-map match source-protocol
    - set routing route-map match source-vrf
    - set routing route-map match tag
    - set routing route-map on-match
    - set routing route-map set-action aggregator
    - set routing route-map set-action as-path exclude
    - set routing route-map set-action as-path prepend
    - set routing route-map set-action atomic-aggregate
    - set routing route-map set-action comm-list-delete
    - set routing route-map set-action community
    - set routing route-map set-action community-additive
    - set routing route-map set-action extcommunity
    - set routing route-map set-action extcommunity bandwidth
    - set routing route-map set-action extcommunity bandwidth-non-transitive
    - set routing route-map set-action ip-next-hop
    - set routing route-map set-action ipv4-vpn-next-hop
    - set routing route-map set-action ipv6-next-hop
    - set routing route-map set-action label-index
    - set routing route-map set-action large-comm-list-delete
    - set routing route-map set-action local-preference
    - set routing route-map set-action metric

    - set routing route-map set-action metric-type
    - set routing route-map set-action origin
    - set routing route-map set-action originator-id
    - set routing route-map set-action src
    - set routing route-map set-action tag
    - set routing route-map set-action weight
- Route Leaking Commands
    - BGP Route Leaking Commands
        - set protocols bgp ipv4-unicast import vrf
        - set protocols bgp ipv6-unicast import vrf
        - set protocols bgp ipv6-unicast import vrf-route-map
        - set protocols bgp vrf ipv4-unicast import vrf
        - set protocols bgp vrf ipv4-unicast import vrf-route-map
        - set protocols bgp vrf ipv6-unicast import vrf
    - Static Route Leaking Commands
        - set protocols static route nexthop-vrf next-hop
        - set protocols static vrf route nexthop-vrf next-hop
- BFD Configuration Commands
    - run show bfd
    - run show bfd counters
    - run show bfd peers
    - set protocols bfd multihop peer local-address
    - set protocols bfd multihop peer local-address detect-multiplier
    - set protocols bfd multihop peer local-address minimum-ttl
    - set protocols bfd multihop peer local-address passive-mode
    - set protocols bfd multihop peer local-address receive-interval
    - set protocols bfd multihop peer local-address shutdown
    - set protocols bfd multihop peer local-address transmit-interval
    - set protocols bfd peer detect-multiplier
    - set protocols bfd peer echo-mode
    - set protocols bfd peer echo receive-interval
    - set protocols bfd peer echo transmit-interval
    - set protocols bfd peer local-address
    - set protocols bfd peer minimum-ttl
    - set protocols bfd peer passive-mode
    - set protocols bfd peer receive-interval
    - set protocols bfd peer shutdown
    - set protocols bfd peer transmit-interval
    - set protocols bfd profile
    - set protocols bfd profile detect-multiplier
    - set protocols bfd profile echo-mode
    - set protocols bfd profile echo receive-interval
    - set protocols bfd profile echo transmit-interval
    - set protocols bfd profile minimum-ttl
    - set protocols bfd profile passive-mode
    - set protocols bfd profile receive-interval
    - set protocols bfd profile shutdown
    - set protocols bfd profile transmit-interval
    - set protocols bgp bfd
    - set protocols ospf6 interface bfd
    - set protocols ospf interface bfd
    - set protocols pim interface bfd
- Policy-Based Routing (PBR) Commands
    - set routing pbr map sequence match destination-ipv4
    - set routing pbr map sequence match source-ipv4
    - set routing pbr map sequence match destination-port
    - set routing pbr map sequence match source-port
    - set routing pbr map sequence match destination-ipv6
    - set routing pbr map sequence match source-ipv6
    - set routing pbr map sequence action nexthop
    - set routing pbr map sequence action dscp
    - set routing pbr map vlan-interface
    - run show pbr map
    - run clear pbr map
- IPv4 Source Guard (IPSG for IPv4) Commands
    - set ip-source-guard binding ip
    - set ip-source-guard enable
    - set ip-source-guard verify
    - set ip-source-guard traceoptions enable
    - run show ip-source-guard binding
- IPv6 Source Guard (IPSG for IPv6) Commands
    - set ipv6-source-guard binding ip

- set ipv6-source-guard enable
- set ipv6-source-guard verify
- set ipv6-source-guard traceoptions enable
- run show ipv6-source-guard binding

- IS-IS commands
  - set protocols isis area-tag network-entity
  - set protocols isis area-tag is-type
  - set protocols isis area-tag interface
  - set protocols isis area-tag hostname-dynamic
  - set protocols isis area-tag area-password authentication-type
  - set protocols isis area-tag area-password authentication-key
  - set protocols isis area-tag area-password authenticate-snp
  - set protocols isis area-tag domain-password authentication-type
  - set protocols isis area-tag domain-password authentication-key
  - set protocols isis area-tag domain-password authenticate-snp
  - set protocols isis area-tag attached-bit receive-ignore
  - set protocols isis area-tag attached-bit send
  - set protocols isis area-tag log-adjacency-changes
  - set protocols isis area-tag metric-style
  - set protocols isis area-tag set-overload-bit
  - set protocols isis area-tag purge-originator
  - set protocols isis area-tag lsp-mtu
  - set protocols isis area-tag lsp-timers gen-interval
  - set protocols isis area-tag lsp-timers refresh-interval
  - set protocols isis area-tag lsp-timers max-lifetime
  - set protocols isis area-tag spf-interval
  - set protocols isis area-tag spf-delay-ietf init-delay
  - set protocols isis area-tag spf-delay-ietf short-delay
  - set protocols isis area-tag spf-delay-ietf long-delay
  - set protocols isis area-tag spf-delay-ietf holddown
  - set protocols isis area-tag spf-delay-ietf time-to-learn
  - set protocols isis area-tag default-information originate
  - set protocols isis area-tag default-information originate metric
  - set protocols isis area-tag default-information originate route-map
  - set protocols isis area-tag topology ipv6-unicast
  - set protocols isis area-tag interface circuit-type
  - set protocols isis area-tag interface csnp-interval
  - set protocols isis area-tag interface psnp-interval
  - set protocols isis area-tag interface hello-padding
  - set protocols isis area-tag interface hello-interval
  - set protocols isis area-tag interface hello-multiplier
  - set protocols isis area-tag interface metric
  - set protocols isis area-tag interface network point-to-point
  - set protocols isis area-tag interface passive
  - set protocols isis area-tag interface password authentication-type
  - set protocols isis area-tag interface password authentication-key
  - set protocols isis area-tag interface priority
  - set protocols isis area-tag interface three-way-handshake
  - set protocols isis area-tag interface bfd
  - set protocols isis area-tag interface topology ipv6-unicast
  - set protocols isis area-tag redistribute
  - set protocols isis traceoption events
  - set protocols isis traceoption adj-packets
  - set protocols isis traceoption route-events
  - set protocols isis traceoption snp-packets
  - run show isis summary
  - run show isis interface
  - run show isis database
  - run show isis hostname
  - run show isis neighbor
  - run show isis route
  - run show isis topology

ACL Configuration Commands

- set firewall filter description
- set firewall filter input interface
- set firewall filter input vlan-interface
- set firewall filter input routed-interface
- set firewall filter output interface
- set firewall filter output vlan-interface

- set firewall filter output routed-interface
- set firewall filter sequence description
- set firewall filter sequence from destination-address-ipv4
- set firewall filter sequence from destination-address-ipv6
- set firewall filter sequence from destination-mac-address
- set firewall filter sequence from destination-port
- set firewall filter sequence from ether-type
- set firewall filter sequence from ip trust-mode
- set firewall filter sequence from ip value
- set firewall filter sequence from protocol icmp
- set firewall filter sequence from protocol igmp
- set firewall filter sequence from protocol ip
- set firewall filter sequence from protocol ospf
- set firewall filter sequence from protocol others
- set firewall filter sequence from protocol tcp
- set firewall filter sequence from protocol tcp flags
- set firewall filter sequence from protocol udp
- set firewall filter sequence from source-address-ipv4
- set firewall filter sequence from source-address-ipv6
- set firewall filter sequence from source-mac-address
- set firewall filter sequence from source-port
- set firewall filter sequence from vlan
- set firewall filter sequence then action
- set firewall filter sequence then forwarding-class
- set firewall filter sequence log interval
- set firewall system-output disable
- set firewall time-range periodic start
- set firewall time-range periodic end
- run show filter
- run show timerange

QoS Configuration Commands

- class-of-service classifier <classifier-name>
- class-of-service classifier <classifier-name> forwarding-class <forwarding-class-name> code-point <code-point>
- class-of-service classifier <classifier-name> trust-mode <trust-mode>
- class-of-service forwarding-class <forwarding-class-name> local-priority <local-priority>
- class-of-service interface <port> classifier <classifier-name>
- class-of-service scheduler <scheduler-name> guaranteed-rate <guaranteed-rate>
- class-of-service scheduler <scheduler-name> mode SP
- class-of-service scheduler <scheduler-name> mode WFQ
- class-of-service scheduler <scheduler-name> mode WRR
- class-of-service scheduler <scheduler-name> weight <weight-id>
- class-of-service scheduler-profile <scheduler-profile-name> forwarding-class <forwarding-class-name> schedule <schedule-name>
- show class-of-service <text>
- set class-of-service interface scheduler-profile
- class-of-service interface <port> default-priority <default-priority-type> <default-priority-int>
- class-of-service pfc-profile <profile-name> code-point <code-point> drop <boolean>
- class-of-service interface <port> pfc-profile <profile-name>
- set firewall filter sequence then dscp
- set class-of-service scheduler max-rate
- CoPP Commands
  - set class-of-service forwarding-class local-priority
  - set class-of-service scheduler max-bandwidth-pps
  - set class-of-service scheduler min-bandwidth-pps
  - set class-of-service scheduler-profile copp-profile forwarding-classs scheduler
  - set class-of-service scheduler weight
  - set firewall filter copp sequence from destination-address-ipv4
  - set firewall filter copp sequence from destination-address-ipv6
  - set firewall filter copp sequence from destination-mac-address
  - set firewall filter copp sequence from destination-port
  - set firewall filter copp sequence from ether-type
  - set firewall filter copp sequence from protocol
  - set firewall filter copp sequence from source-address-ipv4
  - set firewall filter copp sequence from source-address-ipv6
  - set firewall filter copp sequence from source-mac-address
  - set firewall filter copp sequence from source-port
  - set firewall filter copp sequence from vlan
  - set firewall filter copp sequence then forwarding-class
  - set firewall filter copp sequence then dscp
  - run show copp bandwidth

    - run show copp statistics
    - run show filter copp
    - run show interface stm
    - run clear copp statistics
- Buffer Management Commands
    - set interface ethernet-switching-options buffer egress-queue shared-ratio
    - set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared
    - run show gigabit-ethernet egress-queues
    - run show interface egress-buffer
- Interface-based Rate Limiting Commands
    - set interface gigabit-ethernet rate-limiting ingress kilobits
    - set interface gigabit-ethernet rate-limiting ingress ratio
    - set interface gigabit-ethernet rate-limiting ingress burst
    - set interface gigabit-ethernet rate-limiting egress kilobits
    - set interface gigabit-ethernet rate-limiting egress ratio
    - set interface gigabit-ethernet rate-limiting egress burst
- ACL-based Traffic Policer Commands
    - set firewall policer if-exceeding count-mode
    - set firewall policer if-exceeding rate-limit
    - set firewall policer if-exceeding burst-limit
    - set firewall filter sequence then policer
    - set firewall policer if-exceeding action discard
    - run show policer
- PFC Watchdog
    - set class-of-service pfc-watchdog granularity
    - set class-of-service pfc-watchdog restore-action
    - set class-of-service pfc-watchdog code-point detect-interval
    - set class-of-service pfc-watchdog code-point restore-interval
    - set class-of-service interface pfc-watchdog code-point enable
    - run show pfc-watchdog config
    - run show pfc-watchdog stats

Protocol Configuration Commands

- protocols arp aging-time
- set protocols arp interface address mac-address
- set protocols arp interface proxy
- set protocols arp inspection vlan disable
- set protocols arp inspection access-list ip mac-address
- set protocols arp inspection vlan access-list
- set protocols arp inspection trust-port
- run show arp
- run show arp inspection dhcp-binding
- run show arp inspection interface
- run show arp inspection vlan
- run show arp inspection access-list
- run show arp inspection statistics vlan
- protocols lacp interface <interface> priority
- protocols lacp priority
- protocols sflow agent-id
- protocols sflow collector udp-port
- protocols sflow disable
- protocols sflow header-len
- protocols sflow interface <port> disable
- protocols sflow interface <port> header-len
- protocols sflow interface <port> polling-interval
- protocols sflow interface <port> sampling-rate egress
- protocols sflow interface <port> sampling-rate ingress
- protocols sflow polling-interval
- protocols sflow sampling-rate egress
- protocols sflow sampling-rate ingress
- protocols sflow source-address
- set protocols dhcp snooping vlan
- set protocols dhcp snooping trust-port
- set protocols dhcp snooping vlan option82-policy
- set protocols dhcp snooping option82 circuit-id
- set protocols dhcp snooping option82 remote-id
- set protocols dhcp snooping option82 trust-all
- set protocols dhcp snooping binding file
- set protocols dhcp snooping binding write-delay
- run show dhcp snooping binding
- set protocols dhcp relay interface disable

- set protocols dhcp relay interface dhcp-server-address
- set protocols dhcp relay interface relay-agent-address
- set protocols dhcp relay interface option82-policy
- set protocols dhcp relay option82 circuit-id
- set protocols dhcp relay option82 remote-id
- set protocols dhcp relay option82 trust-all
- set protocols dhcp server pool network
- set protocols dhcp server pool range low
- set protocols dhcp server pool range high
- set protocols dhcp server pool domain-name
- set protocols dhcp server pool dns-server
- set protocols dhcp server pool default-router
- set protocols dhcp server pool lease-time
- set protocols dhcp server pool vrf
- run show dhcp server binding address
- run show dhcp server binding interface
- set protocols dhcp6 relay interface disable
- set protocols dhcp6 relay interface destination
- set protocols dhcp6 relay interface remote-id
- run show dhcp6 relay-stats
- set protocols lacp interface rate
- run show lldp neighbor
- set protocols dhcp6 snooping vlan
- set protocols dhcp6 snooping trust-port
- set protocols dhcp6 snooping binding file
- set protocols dhcp6 snooping binding write-delay
- set protocols dhcp6 snooping vlan option-policy
- set protocols dhcp6 snooping option37 remote-id
- set protocols dhcp6 snooping option18 interface-id
- set protocols dhcp6 snooping interface max-clients
- run show dhcp6 snooping binding
- set protocols dhcp6 guard policy device-role
- set protocols dhcp6 guard policy trust-port
- set protocols dhcp6 guard policy interface
- set protocols dhcp6 guard policy preference-min
- set protocols dhcp6 guard policy preference-max
- set protocols dhcp6 guard policy match server source-address
- set protocols dhcp6 guard policy match reply ia-prefix
- run show dhcp6 guard policy
- run show dhcp6 guard

IP Multicast Commands

- IGMP Snooping Configuration Commands
  - run show igmp-snooping
  - run show igmp-snooping groups
  - run show igmp-snooping mrouter
  - run show igmp-snooping querier
  - set protocols igmp-snooping enable
  - set protocols igmp-snooping interface max-groups
  - set protocols igmp-snooping last-member-query-count
  - set protocols igmp-snooping last-member-query-interval
  - set protocols igmp-snooping max-response-time
  - set protocols igmp-snooping query-interval
  - set protocols igmp-snooping report-suppression
  - set protocols igmp-snooping robustness-variable
  - set protocols igmp-snooping vlan-id enable
  - set protocols igmp-snooping vlan-id fast-leave
  - set protocols igmp-snooping vlan-id mrouter interface
  - set protocols igmp-snooping vlan-id querier address
  - set protocols igmp-snooping vlan-id querier enable
  - set protocols igmp-snooping vlan-id querier other-querier-timer
  - set protocols igmp-snooping vlan-id querier version
  - set protocols igmp-snooping vlan-id static group interface
  - set protocols igmp-snooping vlan-id unregistered flood-all
- IGMP Commands
  - set protocols igmp interface
  - set protocols igmp interface join-group
  - set protocols igmp interface query-interval
  - set protocols igmp interface query-max-response-time
  - set protocols igmp interface version

    - run show igmp groups
    - run show igmp interface
- PIM Configuration Commands
    - set protocols pim ecmp
    - set protocols pim interface active-active
    - set protocols pim interface drpriority
    - set protocols pim interface hello holdtime
    - set protocols pim interface hello interval
    - set protocols pim interface sm
    - set protocols pim interface use-source
    - set protocols pim join-prune-interval
    - set protocols pim keep-alive-timer
    - set protocols pim packets
    - set protocols pim register-suppress-time
    - set protocols pim rp
    - set protocols pim spt-switchover infinity-and-beyond
    - set protocols pim ssm prefix-list
    - run show pim interface
    - run show pim rp-info
    - run show pim neighbor
    - run show pim upstream
    - run show mroute
    - mtrace
    - run show pim group-type
- Multicast Source Discovery Protocol (MSDP) Commands
    - set protocols msdp mesh-group source
    - set protocols msdp mesh-group member
    - run show msdp mesh-group
    - run show msdp peer
    - run show msdp sa
- Multicast VLAN Registration (MVR) Commands
    - run show igmp-snooping mvr mvlan
    - run show igmp-snooping mvr receiver-vlan
    - set protocols igmp-snooping vlan-id mvr receiver vlan-list
    - set protocols igmp-snooping vlan-id mvr source group

OpenFlow Commands in CrossFlow Mode

VXLAN Commands

- vxlans source-interface address
- vxlans udp-port
- set vxlans vni <text> decapsulation mode
- vxlans vni <text> encapsulation mode
- vxlans vni <text> encapsulation vlan
- vxlans vni <text> flood vtep
- vxlans vni <text> flood vtep <ipv4-addr> mac-address
- vxlans vni <text> flood vtep <ipv4-addr> traffic-type
- set vxlans vni vlan
- set vxlans tunnel-mac-leaning disable
- OVSDB VTEP command
    - set protocols ovsdb controller <controller-name> address
    - set protocols ovsdb controller <controller-name> inactivity-probe-duration 30000
    - set protocols ovsdb controller <controller-name> maximum-backoff-duration
    - set protocols ovsdb controller <controller-name> port
    - set protocols ovsdb controller c1 protocol
    - set protocols ovsdb interface
    - set protocols ovsdb management-ip
    - set protocols ovsdb ssl bootstrap
    - set protocols ovsdb ssl ca-cert
        - set protocols ovsdb ssl certificate
    - set protocols ovsdb ssl private-key
    - set vxlans ovsdb-managed
    - set protocols ovsdb controller vrf mgmt-vrf
- set vxlans l3-vni prefix-routes-only
- set vxlans l3-vni
- set vxlans vni mcast-group
- run show vxlan statistics
- run clear vxlan statistics
- run show vxlan vni
- run show vxlan address-table

BGP EVPN Commands

- run show bgp evpn route
- run show bgp evpn summary
- run show bgp evpn vni
- run show evpn es
- run show evpn mac vni
- set interface aggregate-ethernet evpn mh es-df-pref
- set interface aggregate-ethernet evpn mh es-id
- set interface aggregate-ethernet evpn mh es-sys-mac
- set l3-interface routed-interface router-mac
- set l3-interface vlan-interface anycast address
- set l3-interface vlan-interface anycast mac
- set l3-interface vlan-interface router-mac
- set protocols bgp evpn advertise-all-vni
- set protocols bgp evpn advertise-default-gw
- set protocols bgp evpn advertise ipv4-unicast
- set protocols bgp evpn advertise ipv6-unicast
- set protocols bgp evpn advertise-svi-ip
- set protocols bgp evpn default-originate
- set protocols bgp evpn disable-ead-evi-rx
- set protocols bgp evpn disable-ead-evi-tx
- set protocols bgp evpn vni
- set protocols bgp evpn vni advertise-default-gw
- set protocols bgp evpn vni advertise-subnet
- set protocols bgp evpn vni advertise-svi-ip
- set protocols bgp evpn vni rd
- set protocols bgp evpn vni route-target type
- set protocols bgp neighbor evpn activate
- set protocols bgp neighbor evpn allowas-in
- set protocols bgp neighbor evpn route-map
- set protocols bgp neighbor evpn route-reflector-client
- set protocols bgp vrf evpn advertise-pip ip
- set protocols evpn mh mac-holdtime
- set protocols evpn mh neigh-holdtime
- set protocols evpn mh redirect-off
- set protocols evpn mh startup-delay
- set vxlans vni arp-nd-suppress disable

PoE Configuration Commands

- set poe interface max-power
- set poe interface detection-type
- set poe interface enable
- set poe interface mode
- set poe interface priority
- set poe interface threshold-mode
- set poe power management-mode
- set poe power mode
- set poe interface lldp-negotiation
- set poe power voltage
- set protocols poe traceoptions flag all disable
- run show poe interface
- run show poe power

VRRP Commands

- set protocols vrrp interface vrid
- set protocols vrrp interface vrid disable
- set protocols vrrp interface vrid version
- set protocols vrrp interface vrid ip
- set protocols vrrp interface vrid priority
- set protocols vrrp interface vrid interval
- set protocols vrrp interface vrid preempt enable
- set protocols vrrp interface vrid load-balance disable
- set protocols vrrp interface vrid load-balance virtual-mac time-interval
- set protocols vrrp interface vrid accept disable
- set protocols vrrp interface vrid authentication type
- set protocols vrrp interface vrid simple-key
- set protocols vrrp interface vrid md5-key
- run show vrrp
- set protocols vrrp interface vrid ipv6-nd adv-interval-option

- set protocols vrrp interface vrid ipv6-nd home-agent-config-flag
- set protocols vrrp interface vrid ipv6-nd home-agent-lifetime
- set protocols vrrp interface vrid ipv6-nd home-agent-preference
- set protocols vrrp interface vrid ipv6-nd managed-config-flag
- set protocols vrrp interface vrid ipv6-nd mtu
- set protocols vrrp interface vrid ipv6-nd other-config-flag
- set protocols vrrp interface vrid ipv6-nd prefix off-link
- set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix router-address
- set protocols vrrp interface vrid ipv6-nd ra-fast-retrans
- set protocols vrrp interface vrid ipv6-nd ra-interval
- set protocols vrrp interface vrid ipv6-nd ra-lifetime
- set protocols vrrp interface vrid ipv6-nd reachable-time
- set protocols vrrp interface vrid ipv6-nd router-preference
- set protocols vrrp interface vrid ipv6-nd suppress-ra

Spanning Tree Protocol Commands

- run show spanning-tree
- run show spanning-tree mstp
- run show spanning-tree pvst
- run show spanning-tree rstp
- run show spanning-tree statistics
- run show spanning-tree stp
- set protocols spanning-tree enable
- set protocols spanning-tree force-version
- set protocols spanning-tree interface enable
- set protocols spanning-tree mstp bridge-priority
- set protocols spanning-tree mstp configuration-name
- set protocols spanning-tree mstp forward-delay
- set protocols spanning-tree mstp hello-time
- set protocols spanning-tree mstp interface bpdu-filter
- set protocols spanning-tree mstp interface bpdu-guard
- set protocols spanning-tree mstp interface edge
- set protocols spanning-tree mstp interface external-path-cost
- set protocols spanning-tree mstp interface internal-path-cost
- set protocols spanning-tree mstp interface manual-forwarding
- set protocols spanning-tree mstp interface mode
- set protocols spanning-tree mstp interface port-priority
- set protocols spanning-tree mstp interface root-guard
- set protocols spanning-tree mstp interface tcn-guard
- set protocols spanning-tree mstp max-age
- set protocols spanning-tree mstp max-hops
- set protocols spanning-tree mstp msti bridge-priority
- set protocols spanning-tree mstp msti interface cost
- set protocols spanning-tree mstp msti interface port-priority
- set protocols spanning-tree mstp msti vlan
- set protocols spanning-tree mstp revision-level
- set protocols spanning-tree pvst interface bpdu-guard
- set protocols spanning-tree pvst interface manual-forwarding
- set protocols spanning-tree pvst interface mode
- set protocols spanning-tree pvst interface root-guard
- set protocols spanning-tree pvst vlan bridge-priority
- set protocols spanning-tree pvst vlan enable
- set protocols spanning-tree pvst vlan forward-delay
- set protocols spanning-tree pvst vlan hello-time
- set protocols spanning-tree pvst vlan interface path-cost
    - set protocols spanning-tree pvst vlan interface port-priority
- set protocols spanning-tree pvst vlan max-age
- set protocols spanning-tree rstp bridge-priority
- set protocols spanning-tree rstp forward-delay
- set protocols spanning-tree rstp hello-time
- set protocols spanning-tree rstp interface bpdu-filter
- set protocols spanning-tree rstp interface bpdu-guard
- set protocols spanning-tree rstp interface edge
- set protocols spanning-tree rstp interface mode
- set protocols spanning-tree rstp interface path-cost
- set protocols spanning-tree rstp interface port-priority
- set protocols spanning-tree rstp interface root-guard
- set protocols spanning-tree rstp interface tcn-guard

- set protocols spanning-tree rstp max-age
- set protocols spanning-tree stp bridge-priority
- set protocols spanning-tree stp forward-delay
- set protocols spanning-tree stp hello-time
- set protocols spanning-tree stp interface bpdu-filter
- set protocols spanning-tree stp interface bpdu-guard
- set protocols spanning-tree stp interface edge
- set protocols spanning-tree stp interface mode
- set protocols spanning-tree stp interface path-cost
- set protocols spanning-tree stp interface port-priority
- set protocols spanning-tree stp interface root-guard
- set protocols spanning-tree stp interface tcn-guard
- set protocols spanning-tree stp max-age

MLAG Commands

- set protocols mlag domain
- set protocols mlag domain node
- set protocols mlag domain interface link
- set protocols mlag domain peer-ip peer-link
- set protocols mlag domain peer-ip peer-vlan
- run show mlag domain
- run show mlag link
- run show mlag consistency-parameter

GRE Tunnel Interface Commands

- run show l3-interface tunnel
- set l3-interface tunnel address
- set l3-interface tunnel destination
- set l3-interface tunnel disable
- set l3-interface tunnel source
- set l3-interface tunnel tunnel-mode gre-ip
- set l3-interface tunnel vrf

GVRP Commands

- set protocols gvrp join-timer
- set protocols gvrp leave-timer
- set protocols gvrp leaveall-timer
- run clear gvrp interface statistics
- run show gvrp interface
- run show gvrp interface statistics
- set protocols gvrp edge-switch
- set protocols gvrp enable
- set protocols gvrp interface enable
- set protocols gvrp traceoptions flag config
- set protocols gvrp traceoptions flag packets

MVRP Commands

- run clear mvrp interface statistics
- run show mvrp interface
- run show mvrp interface statistics
- set protocols mvrp edge-switch
- set protocols mvrp enable
- set protocols mvrp interface enable
- set protocols mvrp traceoptions flag config
- set protocols mvrp traceoptions flag packets
- set protocols mvrp join-timer
- set protocols mvrp leave-timer
- set protocols mvrp leaveall-timer

ERPS Commands

- run show erps brief
- run show erps interface
- run show erps ring
- run show erps statistics
- set protocols erps enable
- set protocols erps ring
- set protocols erps version
- set protocols erps ring instance

- set protocols erps ring instance control-vlan
- set protocols erps ring instance description
- set protocols erps ring instance enable
- set protocols erps ring instance guard-timer
- set protocols erps ring instance holdoff-timer
- set protocols erps ring instance protected-instance
- set protocols erps ring instance r-aps level
- set protocols erps ring instance rpl
- set protocols erps ring instance wtr-timer
- set protocols erps ring port0 interface
- set protocols erps ring port1 interface
- set protocols erps ring r-aps ring-mac
- set protocols erps ring sub-ring
- set protocols erps ring virtual-channel
- set protocols erps ring instance non-revertive
- set protocols erps tcn-propagation
- set protocols erps ring instance connect ring
- erps switch force ring instance
- erps switch manual ring instance
- erps clear ring ring instance
- set protocols erps traceoptions flag all disable
- set protocols erps traceoptions flag config disable
- set protocols erps traceoptions flag ring disable

EFM OAM Commands

- set protocols ethernet-oam interface enable
- set protocols ethernet-oam interface mode
- set protocols ethernet-oam interface remote-loopback supported
- set protocols ethernet-oam interface remote-loopback timeout
- ethernet-oam remote-loopback start|stop interface
- set protocols ethernet-oam interface timeout
- set protocols ethernet-oam traceoptions flag packets
- set protocols ethernet-oam traceoptions flag config
- run show ethernet-oam
- run show ethernet-oam statistics

Loopback Detection Commands

- set protocols loopback-detection enable
- set protocols loopback-detection interface enable
- set protocols loopback-detection message-interval
- set protocols loopback-detection traceoptions configuration disable
- set protocols loopback-detection traceoptions all disable
- run show loopback-detection
- run clear loopback-detection interface

Command-Line Interface Commands

The section provides the commands about command-line interface operation.

- copy running-config startup-config
- set cli idle-timeout
- set cli screen-length
- set cli terminal
- syslog monitor
- syslog notify
- hwclock
- rollback

Since the support for features and protocols may vary across different models, please ensure that the switch model supports the relevant features or protocols when referring to the documentation.

copy running-config startup-config

The **copy running-config startup-config** command saves the running configuration file from the RAM to the flash.

> **Warning:**
>
> This command is supported only on FS S5810 Series, S3410 Series and S5860 Series switches, and you have to do configuration saving by running this command. This specific save command is requested by hardware vendor due to the Flash limitation on numbers of write/erase cycles.

Command Syntax

copy running-config startup-config

Parameter

None.

Usage Guidelines

When performing the following operations, you need to manually issue the configuration saving command to save the configuration file from the RAM to the flash.

- Perform picos_boot
- Set L2 / L3 CLI commands (for the L2 / L3 CLI configuration, you need to issue the **commit** command before saving the configuration to flash)
- Set OVS commands
- Set CrossFlow commands

You can use either one of the following two methods to save your configuration, using the **save_config** command or the **copy running-config startup-config** command:

- Method 1: Under Linux bash, issue the following command manually (When setting OVS commands, you can only use this command to save the configuration file):

```
admin@Xorplus$ sudo save_config
```

- Method 2: In the L2/L3 CLI operating mode, issue the following command manually:

```
admin@Xorplus> copy running-config startup-config
```

Example

- Save the running configuration file from the RAM to the flash after setting the L2 / L3 CLI commands.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 disable true
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2
admin@Xorplus# commit
Merging the configuration.
Commit OK.
Save done.
admin@Xorplus# quit
admin@Xorplus> copy running-config startup-config
```

set cli idle-timeout

To set the maximum idle time before the current session is terminated, use the **set cli idle-timeout** command in L2/L3 operation mode.

Command Syntax

set cli idle-timeout *time*

Parameters

time	The maximum idle time before the terminal session is terminated. The range is from 0 to 2,000,000 seconds.

Examples

This example demonstrates how to set the maximum idle time to 900 seconds (15 minutes):

```
admin@Switch> set cli idle-timeout 900
```

set cli screen-length

To set the number of lines of output to display on the terminal screen for the current session before pausing, use the **set cli screen-length** command in L2/L3 operation mode.

Command Syntax

set cli screen-length *lines*

Parameters

lines	Number of lines to display. The range is from 0 to 10,000. Use 0 to not pause while displaying output.

Examples

This example shows how to set the number of lines of command output to display on the terminal before pausing:

```
admin@Switch> set cli screen-length 25
```

set cli terminal

To specify the type of terminal for the current session, use the **set cli terminal** command in L2/L3 operation mode.

Command Syntax

set cli terminal { **ansi** | **linux** | **vt100** | **xterm** }

Examples

This example shows how to set the terminal type to **linux** for the current session:

```
admin@Switch> set cli terminal linux
```

syslog monitor

The **syslog monitor** command configures whether to enable or disable the syslog monitor function.

Command Syntax

syslog monitor <**on** | **off**>

Parameter

Parameter	Description
on | off	Enable or disable the syslog monitor function. The value could be **on** or **off**. • **on**: enables the syslog monitor function. • **off**: disables the syslog monitor function. The default value is **off**.

Usage Guidelines

By configuring the syslog monitor function, you can view system log information on the user terminal (including host from which you log in to the device through the console interface) to monitor the running status of the device.

NOTE:

You can configure this command either in Linux shell or CLI mode as shown below:

- From the "**>**" prompt, use the following format,

  admin@Xorplus> syslog monitor on
- From the "**#**" prompt, use the following format,

  admin@Xorplus# run syslog monitor on

Example

- Enable the syslog monitor function.

```
admin@Xorplus> syslog monitor on
```

- Disable the syslog monitor function.

```
admin@Xorplus> syslog monitor off
```

syslog notify

The **syslog notify** command configures whether to enable or disable the function of multi-window command configuration display on the user terminal.

Command Syntax

syslog notify <**on | off**>

Parameter

Parameter	Description
on | off	Enable or disable multi-window command configuration display on the user terminal. The value is **on** or **off**. **on**: enables command configuration display on the user terminal. **off**: disables command configuration display on the user terminal. The default value is **on**.

Usage Guidelines

The CLI window will not synchronously print the configurations of the same switch from other CLI windows to the current CLI interface if disables the function of multi-window command configuration on the user terminal.

The function is window dependent, that is, it will take effect based on CLI windows regardless of the CLI login method (Console or SSH) or the login IP of terminal or the login users.

When the window is restarted, the configuration of multi-window command configuration display on the user terminal function will go to the default value.

NOTE:

You can configure this command either in Linux shell or CLI mode as shown below:

- From the ">" prompt, use the following format,

  admin@Xorplus> syslog notify on
- From the "#" prompt, use the following format,

  admin@Xorplus# run syslog notify on

Example

- Enable the function of multi-window command configuration display on the user terminal.

```
admin@Xorplus> syslog notify on
```

- Disable the function of multi-window command configuration display on the user terminal.

```
admin@Xorplus> syslog notify off
```

hwclock

hwclock is an administration tool for the time clocks. It can display the Hardware Clock time and set the Hardware Clock. Run the command with *sudo* before it, or by *root* user, as it can be executed only by the superuser.

Command Syntax

Under Linux bash, use the following format,

hwclock [*function*] [*option...*]

Parameter

Parameter	Description
function:	
-h, --help	Show help text and exit.
-r, --show	Read hardware clock and print result.
--set	Set the RTC to the time given with –date.
-s, --hctosys	Set the system time from the hardware clock.
-w, --systohc	Set the hardware clock from the current system time.
--systz	Set the system time based on the current timezone.
--adjust	Adjust the RTC to account for systematic drift since the clock was last set or adjusted.
--getepoch	Print out the kernel's hardware clock epoch value.
--setepoch	Set the kernel's hardware clock epoch value to the value given with –epoch.
--predict	Predict RTC reading at time given with –date.
-V, --version	Display version information and exit.
*option***:**	
-u, --utc	The hardware clock is kept in UTC.
--localtime	The hardware clock is kept in local time.
-f, --rtc <file>	Special /dev/... file to use instead of default.
--directisa	Access the ISA bus directly instead of /dev/rtc.
--badyear	Ignore RTC's year because the BIOS is broken.
--date <time>	Specifies the time to set the hardware clock to.
--epoch <year>	Specifies the year which is the beginning of the hardware clock's epoch value.
--noadjfile	Do not access /etc/adjtime; this requires the use of either --utc or –localtime.
--adjfile <file>	Specifies the path to the adjust file; the default is /etc/adjtime.
--test	Do not update anything, just show what would happen.
-D, --debug	Debugging mode.

Example

- Show the help information of hwclock command.

```
admin@193:/$ sudo hwclock -h
Usage:
 hwclock [function] [option...]

Functions:
 -h, --help           show this help text and exit
```

```
 -r, --show           read hardware clock and print result
     --set            set the RTC to the time given with --date
 -s, --hctosys        set the system time from the hardware clock
 -w, --systohc        set the hardware clock from the current system time
     --systz          set the system time based on the current timezone
     --adjust         adjust the RTC to account for systematic drift since
                        the clock was last set or adjusted
     --getepoch       print out the kernel's hardware clock epoch value
     --setepoch       set the kernel's hardware clock epoch value to the
                        value given with --epoch
     --predict        predict RTC reading at time given with --date
 -V, --version        display version information and exit

Options:
 -u, --utc            the hardware clock is kept in UTC
     --localtime      the hardware clock is kept in local time
 -f, --rtc <file>     special /dev/... file to use instead of default
     --directisa      access the ISA bus directly instead of /dev/rtc
     --badyear        ignore RTC's year because the BIOS is broken
     --date <time>    specifies the time to which to set the hardware clock
     --epoch <year>   specifies the year which is the beginning of the
                        hardware clock's epoch value
     --noadjfile      do not access /etc/adjtime; this requires the use of
                        either --utc or --localtime
     --adjfile <file> specifies the path to the adjust file;
                        the default is /etc/adjtime
     --test           do not update anything, just show what would happen
 -D, --debug          debugging mode
```

- Display hardware clock time.

```
admin@193:/$ sudo hwclock --show
Thu Jan 11 21:51:15 2001  -0.719120 seconds
```

rollback

The **rollback** command can be used to rollback the configuration.

Command Syntax

rollback <0 | 1 | 2 |3 | 4 | 5 | default>

Usage Guidelines

Each time a configuration in L2/L3 is commited, a rollback configuration file is created. For example, if configuration is committed five times, **pica.conf.01** through **pica.conf.05** are created. User can rollback to any of these configurations when necessary. The maximum quantity of rollback files is limited to five. The current configuration is located in ***pica.conf***. “rollback 0" refers to load the configurations in file ***pica.conf.***

The **rollback default** command completely replaces the running configuration with the default configuration file. After this command is executed, a commit is required to make the rollback to default configuration take effect.

Warning: This command should be used with caution. All the user configurations will be overridden by the default configurations.

Example

- Rollback the configuration to in configuration file **pica.conf.01**.

```
admin@XorPlus# rollback 1
admin@XorPlus# Loading config file...
Config file was loaded successfully.
admin@XorPlus# commit
Commit OK.
Save done.
```

System Management Commands

- NAC Configuration Commands
  - set protocols dot1x aaa radius authentication server-ip
  - set protocols dot1x aaa radius authentication server-ip priority
  - set protocols dot1x aaa radius authentication server-ip retry-num
  - set protocols dot1x aaa radius authentication server-ip retry-interval
  - set protocols dot1x aaa radius authentication server-ip detect-interval
  - set protocols dot1x interface auth-mode 802.1x
  - set protocols dot1x interface auth-mode 802.1x fallback-to-web disable
  - set protocols dot1x interface auth-mode mac-radius
  - set protocols dot1x interface auth-mode web
  - set protocols dot1x interface authentication-open disable
  - set protocols dot1x aaa radius dynamic-author client
  - set protocols dot1x aaa radius dynamic-author client shared-key
  - set protocols dot1x aaa radius nas-ip
  - set protocols dot1x aaa radius accounting disable
  - set protocols dot1x interface host-mode
  - set protocols dot1x block-vlan-id
  - set protocols dot1x server-fail-vlan-id
  - set protocols dot1x filter sequence from destination-address-ipv4
  - set protocols dot1x filter sequence from destination-address-ipv6
  - set protocols dot1x filter sequence from destination-port
  - set protocols dot1x filter sequence from ether-type
  - set protocols dot1x filter sequence from source-address-ipv4
  - set protocols dot1x filter sequence from source-address-ipv6
  - set protocols dot1x filter sequence from source-port
  - set protocols dot1x filter sequence from protocol
  - set protocols dot1x filter sequence then action
  - run show dot1x all
  - run show dot1x interface
  - run show dot1x server
  - run show dot1x dynamic filter
  - run show dot1x downloadable filter
  - run show dot1x interface statistics gigabit-ethernet
  - set protocols dot1x server-fail recovery-method
  - set protocols dot1x aaa radius authentication server-ip consecutive-detect-num
  - set protocols dot1x aaa vrf mgmt-vrf
  - set protocols dot1x interface session-timeout
  - set protocols dot1x interface recovery-timeout
  - set protocols dot1x server-fail recovery-timeout
  - set protocols dot1x interface max-sessions
  - set protocols dot1x max-sessions-per-port
  - set protocols dot1x aaa radius authentication server-ip auth-port
  - set protocols dot1x aaa radius authentication server-ip acct-port
  - set protocols dot1x aaa radius dynamic-author client port
  - run show dot1x radius-port
  - set protocols dot1x filter sequence from destination-mac-address
  - set protocols dot1x filter sequence from vlan
- SNMP Configuration Commands
  - set protocols snmp trap-group targets security-name
  - set protocols lldp snmp-trap
  - set protocols snmp trap-group event cpu-threshold enable
  - set protocols snmp trap-group event cpu-threshold high
  - set protocols snmp trap-group event cpu-threshold interval
  - set protocols snmp trap-group event cpu-threshold low
  - set protocols snmp trap-group event mac-threshold enable
  - set protocols snmp trap-group event mac-threshold interval
  - set protocols snmp trap-group event mac-threshold limit
  - set protocols snmp trap-group vrf mgmt-vrf
  - set protocols snmp trap-group version
  - set protocols snmp v3 enable
  - set protocols snmp v3 usm-user

    - set protocols snmp v3 usm-user group
    - set protocols snmp v3 group notify-view
    - set protocols snmp v3 group read-view
    - set protocols snmp v3 group write-view
    - set protocols snmp v3 group security-level
    - set protocols snmp v3 usm-user authentication-mode
    - set protocols snmp v3 usm-user authentication-key
    - set protocols snmp v3 usm-user privacy-mode
    - set protocols snmp v3 usm-user privacy-key
    - set protocols snmp v3 mib-view subtree mask
    - set protocols snmp v3 mib-view subtree type
    - set protocols snmp trap-group source-interface
    - set protocols snmp community
    - set protocols snmp community authorization
    - set protocols snmp community clients
    - set protocols snmp contact
    - set protocols snmp location
    - run show snmp statistics
- Mirror Configuration Commands
    - set interface ethernet-switching-options analyzer input
    - set interface ethernet-switching-options analyzer output
    - set interface ethernet-switching-options analyzer erspan input
    - set interface ethernet-switching-options analyzer erspan output source-ip
    - set interface ethernet-switching-options analyzer erspan output dest-ip
    - set interface ethernet-switching-options analyzer erspan output vrf
    - run show analyzer
    - set firewall filter sequence then erspan source-ip
    - set firewall filter sequence then erspan dest-ip
    - set firewall filter sequence then erspan vrf
    - set firewall filter sequence then erspan ttl
- RMON Commands
    - run show rmon alarms
    - run show rmon eventlog
    - run show rmon events
    - run show rmon history
    - run show rmon statistics
    - set protocols snmp rmon alarm falling-event-index
    - set protocols snmp rmon alarm falling-threshold
    - set protocols snmp rmon alarm interval
    - set protocols snmp rmon alarm owner
    - set protocols snmp rmon alarm rising-event-index
    - set protocols snmp rmon alarm rising-threshold
    - set protocols snmp rmon alarm sample-type
    - set protocols snmp rmon alarm variable
    - set protocols snmp rmon event community
    - set protocols snmp rmon event description
    - set protocols snmp rmon event owner
    - set protocols snmp rmon event type
    - set protocols snmp rmon history buckets
    - set protocols snmp rmon history interface
    - set protocols snmp rmon history interval
    - set protocols snmp rmon history owner
    - set protocols snmp rmon statistics interface
    - set protocols snmp rmon statistics owner
- RESTCONF Commands
    - set protocols restconf
    - set protocols restconf port
    - set protocols restconf traceoptions flag config disable
    - set protocols restconf traceoptions flag all disable
    - set protocols restconf traceoptions flag datastore disable
- run show system boot-messages
- run show system connections
- run show system core-dumps
- run show system cpu-usage
- run show system date
- run show system fan
- run show system memory-usage
- run show system name
- run show system ntp-status
- run show system os
- run show system processes brief

- run show system processes detail
- run show system rollback compare to
- run show system rollback file
- run show system rollback list
- run show system rpsu
- run show system serial-number
- run show system temperature
- run show system uptime
- run show system users
- set system aaa local disable
- set system aaa radius accounting disable
- set system aaa radius accounting server-ip
- set system aaa radius accounting server-ip port
- set system aaa radius accounting server-ip shared-key
- set system aaa radius accounting server-ip timeout
- set system aaa radius authorization disable
- set system aaa radius authorization server-ip
- set system aaa radius authorization server-ip port
- set system aaa radius authorization server-ip shared-key
- set system aaa radius authorization server-ip timeout
- set system aaa radius vrf mgmt-vrf
- set system aaa tacacs-plus accounting
- set system aaa tacacs-plus authorization
- set system aaa tacacs-plus auth-type
- set system aaa tacacs-plus disable
- set system aaa tacacs-plus key
- set system aaa tacacs-plus port-number
- set system aaa tacacs-plus timeout
- set system aaa tacacs-plus server-ip
- set system aaa tacacs-plus source-interface
- set system aaa local-auth-fallback disable
- set system aaa tacacs-plus vrf mgmt-vrf
- set system hostname
- set system inband vlan-interface
- set system inband loopback
- set system inband routed-interface
- set system inband enable
- system login-acl network
- system login announcement
- system login user
- system login user admin class
- set system login user authentication plain-text-password
- system login user class
- set system timezone
- set system ntp server-ip
- set system ntp source-interface
- set system ntp vrf mgmt-vrf
- set interface gigabit-ethernet ptp mode
- set system services ssh connection-limit
- set system services ssh disable
- set system services ssh protocol-version v2
- set system services ssh rate-limit
- set system services ssh root-login
- set system services ssh idle-timeout
- set system services ssh port
- set system snmp-acl security-name network
- set system syslog server-ip
- set system syslog local-file
- set system syslog vrf mgmt-vrf
- set system usb disable
- set system management-ethernet eth0 ip-address {IPv4 | IPv6}
- set system management-ethernet eth0 ip-gateway {IPv4 | IPv6}
- show system management-ethernet
- run request system reboot
- run show system hwinfo
- ping
- traceroute
- tftp
- set protocols sflow collector vrf mgmt-vrf
- scp
- set system login banner

- upgrade2 image-file
- upgrade2 image-file backup-file
- upgrade2 image-file factory-default
- upgrade2 image-file use-prev-config
- set system dns-server-ip
- set system console idle-timeout
- set system login multiline-banner message
- set system login multiline-announcement message
- set system aaa radius source-interface
- set protocols grpc enable
- set protocols grpc port
- set system ztp enable
- telnet
- set system start-shell-sh password
- set system services telnet disable

NAC Configuration Commands

- set protocols dot1x aaa radius authentication server-ip
- set protocols dot1x aaa radius authentication server-ip priority
- set protocols dot1x aaa radius authentication server-ip retry-num
- set protocols dot1x aaa radius authentication server-ip retry-interval
- set protocols dot1x aaa radius authentication server-ip detect-interval
- set protocols dot1x interface auth-mode 802.1x
- set protocols dot1x interface auth-mode 802.1x fallback-to-web disable
- set protocols dot1x interface auth-mode mac-radius
- set protocols dot1x interface auth-mode web
- set protocols dot1x interface authentication-open disable
- set protocols dot1x aaa radius dynamic-author client
- set protocols dot1x aaa radius dynamic-author client shared-key
- set protocols dot1x aaa radius nas-ip
- set protocols dot1x aaa radius accounting disable
- set protocols dot1x interface host-mode
- set protocols dot1x block-vlan-id
- set protocols dot1x server-fail-vlan-id
- set protocols dot1x filter sequence from destination-address-ipv4
- set protocols dot1x filter sequence from destination-address-ipv6
- set protocols dot1x filter sequence from destination-port
- set protocols dot1x filter sequence from ether-type
- set protocols dot1x filter sequence from source-address-ipv4
- set protocols dot1x filter sequence from source-address-ipv6
- set protocols dot1x filter sequence from source-port
- set protocols dot1x filter sequence from protocol
- set protocols dot1x filter sequence then action
- run show dot1x all
- run show dot1x interface
- run show dot1x server
- run show dot1x dynamic filter
- run show dot1x downloadable filter
- run show dot1x interface statistics gigabit-ethernet
- set protocols dot1x server-fail recovery-method
- set protocols dot1x aaa radius authentication server-ip consecutive-detect-num
- set protocols dot1x aaa vrf mgmt-vrf
- set protocols dot1x interface session-timeout
- set protocols dot1x interface recovery-timeout
- set protocols dot1x server-fail recovery-timeout
- set protocols dot1x interface max-sessions
- set protocols dot1x max-sessions-per-port
- set protocols dot1x aaa radius authentication server-ip auth-port
- set protocols dot1x aaa radius authentication server-ip acct-port
- set protocols dot1x aaa radius dynamic-author client port
- run show dot1x radius-port
- set protocols dot1x filter sequence from destination-mac-address
- set protocols dot1x filter sequence from vlan

set protocols dot1x aaa radius authentication server-ip

The **set protocols dot1x aaa radius authentication server-ip** command configures the IP address and shared key of the RADIUS authentication server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **shared-key** <*key-string*>

Parameter

Parameter	Description
server-ip <*ip-address*>	Specifies IPv4 address of RADIUS authentication server.
shared-key <*key-string*>	Specifies the shared key of RADIUS authentication server. The value is a string type. Note: The value of shared key should be the same as that on the RADIUS authentication server.

Usage Guidelines

The AAA RADIUS authentication server is used in NAC authentication, including 802.1X authentication, MAB authentication, CWA authentication, Downloadable ACL and Dynamic ACL functions, exchanges RADIUS packet with the switch. Note that up to 20 AAA RADIUS servers can be configured on the switch. The server with the smallest IP address and reachable is used for NAC authentication.

Example

- Configure the IP address and shared key of the 802.1X RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 shared-key pica8abc
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip priority

The **set protocols dot1x aaa radius authentication server-ip** priority command configures the priority of the AAA RADIUS authentication server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **priority** <*priority*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
priority <*priority*>	Specifies the priority of RADIUS authentication server. The value is an integer that ranges from 1 to 20. Priority of 1 is higher than 20. If the priority is not specified for a AAA server, the default priority is infinity, indicating a lowest priority.

Usage Guidelines

Note: Up to 20 AAA RADIUS servers can be configured on the switch.

If several AAA RADIUS servers have been deployed, users can specify different priority for different server by using this command. AAA RADIUS server with higher priority is selected for NAC authentication.

If two servers have the same priority, the server with the smallest IP address and reachable will be used for NAC authentication.

Example

- Configure the priority of the AAA RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 priority 2
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip retry-num

The **set protocols dot1x aaa radius authentication server-ip retry-num** command configures the maximum number of authentication attempts when the AAA server does not respond during NAC authentication.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **retry-num** <*retry-num*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
retry-num <*retry-num*>	Specifies the maximum number of authentication attempts. The value is an integer that ranges from 1 to 5. The default value is 3.

Usage Guidelines

When performing NAC authentication, if the AAA server does not respond to the switch, switch sends authentication message to the AAA server for several times. Use this command to configure the maximum number of authentication attempts, use another command set protocols dot1x aaa radius authentication server-ip <ipv4-address> **retry-interval** <*retry-interval*> to configure the interval for re-sending the authentication messages.

If the AAA server still does not respond after trying the times of **retry-num**, the AAA server is considered inaccessible. If all the AAA servers are inaccessible, the access port of the client will be added to the server fail VLAN, and the packets from the client can only be forwarded in this VLAN.

Example

- Configure the maximum number of authentication attempts to 2.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 retry-num 2
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip retry-interval

The **set protocols dot1x aaa radius authentication server-ip retry-interval** command configures the interval for re-sending the authentication messages to the AAA server when the AAA server does not respond during NAC authentication.

Command Syntax

set protocols dot1x aaa radius authentication server-ip *<ipv4-address>* **retry-interval** *<retry-interval>*

Parameter

Parameter	Description
server-ip *<ipv4-address>*	Specifies IPv4 address of RADIUS authentication server.
retry-interval *<retry-interval>*	Specifies the interval for re-sending the authentication messages. The value is an integer that ranges from 1 to 5, in seconds. The default value is 1s.

Usage Guidelines

When performing NAC authentication, if the AAA server does not respond to the switch, switch re-sends authentication message to the AAA server for several times. Use command set protocols dot1x aaa radius authentication server-ip <ipv4-address> **retry-num** *<retry-num>* to configure the maximum number of authentication attempts, use command set protocols dot1x aaa radius authentication server-ip <ipv4-address> **retry-interval** *<retry-interval>* to configure the interval for re-sending the authentication messages.

If the AAA server still does not respond after trying the times of **retry-num**, it is considered inaccessible. If all the AAA servers are inaccessible, the access port of the client will be added to the server fail VLAN, and the packets from the client can only be forwarded in this VLAN.

Example

- Configure the interval for re-sending the authentication messages.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 retry-interval 3
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip detect-interval

The **set protocols dot1x aaa radius authentication server-ip detect-interval** command configures the detection interval of the AAA RADIUS authentication server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **detect-interval** <*detect-interval*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
detect-interval <*detect-interval*>	Specifies the detection interval. The value is an integer that ranges from 0 to 300, in seconds, where “0” indicates disabling detect function. The default value is 5s.

Usage Guidelines

After a AAA server is configured, the switch sends Test Radius Request detection message to the server to detect the reachability of the AAA server. If the AAA server is not reachable, switch will re-send the Test Radius Request message again after the detection interval to detect the reachability of the AAA server until the AAA server is reachable.

Example

- Configure the detection interval of the AAA RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 detect-interval 10
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode 802.1x

The **set protocols dot1x interface auth-mode 802.1x** command enables the 802.1X authentication mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode 802.1x**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When no NAC authentication mode and the CLI command **set protocols dot1x interface** <*interface-name*> are configured, the port is open to the user; but if the CLI command **set protocols dot1x interface** <*interface-name*> is configured, the port becomes blocked.

802.1X authentication is an authentication method that controls the network access rights of users based on ports together with the MAC address of client. The Extensible Authentication Protocol (EAP) packet is used to exchange authentication information between the supplicant, authenticator and authentication server. This technology is mainly used in networks with high security requirements. 802.1X authentication requires 802.1X client software to be installed on the supplicant.

Example

- Enable 802.1X authentication mode on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode 802.1x
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode 802.1x fallback-to-web disable

The **set protocols dot1x interface auth-mode 802.1x fallback-to-web disable** command enables or disables fallback to WEB function.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode 802.1x fallback-to-web disable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
disable <**true**	**false**>	Enables or disables fallback to WEB function. The value could be **true** or **false**. • **true:** disables fallback to WEB function. • **false:** enables fallback to WEB function. By default, fallback to WEB function is disabled.

Example

- Enable fallback to WEB function on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode 802.1x fallback-to-web disable false
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode mac-radius

The **set protocols dot1x interface auth-mode mac-radius** command enables the MAB authentication mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode mac-radius**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When no NAC authentication mode and the CLI node **set protocols dot1x interface** <*interface-name*> are configured, the port is open to the user; but if the CLI node **set protocols dot1x interface** <*interface-name*> is configured, the port becomes blocked.

During the MAB authentication process, the user is not required to manually enter a username or password. The user's MAC address will be encapsulated as user name and password in the packet and sent to the RADIUS server. The port will be opened to the user with this MAC only if it passes the MAB authentication. This technology is suitable for environments where the MAC address is fixed and the security requirements are not very high. At the same time, it can meet the authentication requirements of terminals such as printers that cannot install the authentication client software.

When both 802.1X authentication and MAB authentication modes are enabled, the 802.1X authentication will take precedence over MAB. If the Supplicant supports 802.1x authentication, the system performs 802.1x authentication. Else if the Supplicant does not support 802.1x authentication, the system performs MAB authentication. For the former case, no matter whether 802.1x authentication is successful or not, the MAB authentication process will not be taken.

Example

- Enable MAB authentication mode on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode mac-radius
admin@Xorplus# commit
```

set protocols dot1x interface auth-mode web

The **set protocols dot1x interface auth-mode web** command enables the Web authentication mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **auth-mode web**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When no NAC authentication mode and the CLI command **set protocols dot1x interface** <*interface-name*> are configured, the port is open to the user; but if the CLI command **set protocols dot1x interface** <*interface-name*> is configured, the port becomes blocked.

Example

- Enable Web authentication mode on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 auth-mode web
admin@Xorplus# commit
```

set protocols dot1x interface authentication-open disable

The **set protocols dot1x interface authentication-open disable** command enables open authentication function on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **authentication-open disable <true | false>**

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
disable <true | false>	Configures whether to enable or disable the open authentication function. The value is **true** or **false**. • **true**: disables the open authentication function. • **false**: enables the open authentication function. The default value is **true**.

Usage Guidelines

With open authentication function, only DHCP packets are allowed on the specified port to make Client could get IP address before any authentication has succeeded.

Example

- Enable the open authentication function on ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 authentication-open disable false
```

set protocols dot1x aaa radius dynamic-author client

The **set protocols dot1x aaa radius dynamic-author client** command configures IP address of the RADIUS dynamic authorization client (DAC) for Change of Authorization (CoA) function.

RADIUS dynamic authorization client could be the same RADIUIS authentication server configured in **set protocols dot1x aaa radius authentication server-ip** <*ip-address*> [**shared-key** <*key-string*>] command or it could be a different one.

> **NOTE:**
>
> PICOS supports to configure a maximum of 20 CoA dynamic authorization clients.

Command Syntax

set protocols dot1x aaa radius dynamic-author client <*client-ip*>

Parameter

Parameter	Description
client <*client-ip*>	Specifies the IP address of the RADIUS dynamic authorization client. This component often resides on the RADIUS server.

Example

- Configure the client for CoA function.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 10.10.10.1
admin@Xorplus# commit
```

set protocols dot1x aaa radius dynamic-author client shared-key

The **set protocols dot1x aaa radius dynamic-author client shared-key** command configures the IP address and the shared key of the RADIUS dynamic authorization client (DAC) for Change of Authorization (CoA) function.

NOTE:

This command is supported from PICOS 2.11.16.

Command Syntax

set protocols dot1x aaa radius dynamic-author client <*client-ip*> **shared-key** <*key-string*>

Parameter

Parameter	Description
client <*client-ip*>	Specifies the IP address of the RADIUS dynamic authorization client. This component often resides on the RADIUS authentication server.
shared-key <*key-string*>	Specifies the shared key of the RADIUS dynamic authorization client. The value is a string type. Note: The value of shared key should be the same as the one configured on the RADIUS dynamic authorization client.

Example

- Configure the IP address and the shared key of the RADIUS dynamic authorization client.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 10.10.10.1 shared-key pica8123
admin@Xorplus# commit
```

set protocols dot1x aaa radius nas-ip

The **set protocols dot1x aaa radius nas-ip** command configures the NAS IP address to the interface IP which connected to the RADIUS server.

Command Syntax

set protocols dot1x aaa radius nas-ip <*ip-address*>

Parameter

Parameter	Description
nas-ip <*ip-address*>	Specifies the NAS IP address to the interface IP which connected to the RADIUS server.

Usage Guidelines

This command is to set the nas-ip field in RADIUS access-request message. The value of the NAS IP address depends on the port connected to the RADIUS authentication server:

- If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.
- If you use the L3 VLAN interface, loopback interface, routed interface or sub-interface to connect to the RADIUS server, the IP address of the L3 VLAN interface, loopback interface, routed interface or sub-interface should be used for the NAS IP address configured here.

Example

- Configure the NAS IP address to the interface IP which connected to the RADIUS server.

```
admin@Xorplus# set protocols dot1x aaa radius nas-ip 10.10.10.100
admin@Xorplus# commit
```

set protocols dot1x aaa radius accounting disable

The **set protocols dot1x aaa radius accounting disable** command enables or disables user accounting function when performing NAC authentication.

NOTE:

RADIUS accounting applies only to 802.1X and MAB authentication procedures.

Command Syntax

set protocols dot1x aaa radius accounting disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Enables or disables user accounting function when performing NAC authentication. The value could be **true** or **false**. • **true:** disables user accounting function. • **false:** enables user accounting function. By default, user accounting function is enabled.

Example

- Enable user accounting function when performing NAC authentication.

```
admin@Xorplus# set protocols dot1x aaa radius accounting disable false
admin@Xorplus# commit
```

set protocols dot1x interface host-mode

The **set protocols dot1x interface host-mode** command configures host access mode on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **host-mode** <**single** | **multiple**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
host-mode <**single** | **multiple**>	Specifies host access mode. The value could be **single** or **multiple**. • **Single:** Only one user is allowed to access the switch port, unless the user goes offline other users cannot try to access the port. The authentication will be restarted if port is bounced or client is changed. • **Multiple:** T Multiple clients connect to the network through the same switch port. If a user goes offline, the network access rights of other users are not affected. At most 8 clients are allowed to be authenticated on a single switch port, the ninth will be added into the pending list. The default host mode is **single**. Note that changing host mode from CLI will cause re-authentication for all online users of the port.

Usage Guidelines

This command is to set the nas-ip field in RADIUS access-request message. The value of the NAS IP address depends on the port connected to the RADIUS authentication server:

- If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.
- If you use the L3 VLAN interface to connect to the RADIUS server, the IP address of the L3 VLAN interface should be used for the NAS IP address configured here.

Example

- Configure the host access mode as multiple on interface ge-1/1/1.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 host-mode multiple
admin@Xorplus# commit
```

set protocols dot1x block-vlan-id

The **set protocols dot1x block-vlan-id** command configures block VLAN ID.

Command Syntax

set protocols dot1x block-vlan-id <*vlan-id*>

Parameter

Parameter	Description
block-vlan-id <*vlan-id*>	Specifies the VLAN ID for block VLAN. The value is an integer that ranges from 2 to 4094.

Example

- Configure the block VLAN ID to 100.

```
admin@Xorplus# set protocols dot1x block-vlan-id 100
admin@Xorplus# commit
```

set protocols dot1x server-fail-vlan-id

The **set protocols dot1x server-fail-vlan-id** command configures a server fail VLAN.

Command Syntax

set protocols dot1x server-fail-vlan-id <*vlan-id*>

Parameter

Parameter	Description
server-fail-vlan-id <*vlan-id*>	Specifies the VLAN ID for a server fail VLAN. The value is an integer that ranges from 2 to 4094.

Example

- Configure the server fail VLAN ID to 200.

```
admin@Xorplus# set protocols dot1x server-fail-vlan-id 200
admin@Xorplus# commit
```

set protocols dot1x filter sequence from destination-address-ipv4

The **set protocols dot1x filter sequence from destination-address-ipv4** command configures the destination IPv4 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from destination-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-address-ipv4 <*ipv4-address*>	Specifies the destination IPv4 address of packets that match ACL rules. It must be an IPv4 subnet in address/prefix-length form. For example, 10.1.1.0/24.

Example

- Configure the destination IPv4 address of packets that match ACL rules to 10.1.1.0/24.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-address-ipv4 10.1.1.0/24
admin@Xorplus# commit
```

set protocols dot1x filter sequence from destination-address-ipv6

The **set protocols dot1x filter sequence from destination-address-ipv6** command configures the destination IPv6 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from destination-address-ipv6** <*ipv6-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-address-ipv6 <*ipv6-address*>	Specifies the destination IPv6 address of packets that match ACL rules. It must be an IPv6 subnet in address/prefix-length form. For example, 10::1/128.

Example

- Configure the destination IPv6 address of packets that match ACL rules to 10::1/128.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-address-ipv6 10::1/128
admin@Xorplus# commit
```

set protocols dot1x filter sequence from destination-port

The **set protocols dot1x filter sequence from destination-port** command configures the destination port information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from destination-port** <*port-number*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-port <*port-number*>	Specifies the destination port of packets that match ACL rules. The value is an integer. It could be a port number or a range of port number, i.e. 6000; 6000..7000, which indicates port range from 6000 to 7000.

Example

- Configure the destination port of packets that match ACL rules to 6000.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-port 6000
admin@Xorplus# commit
```

set protocols dot1x filter sequence from ether-type

The **set protocols dot1x filter sequence from ether-type** command configures the Ethernet type information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from ether-type** <*ether-type*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
ether-type <*ether-type*>	Specifies the Ethernet type of packets that match ACL rules. The value is an integer in decimal format that ranges from 1501 to 65535.

Example

- Configure the Ethernet type of packets that match ACL rules to 4525.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from ether-type 4525
admin@Xorplus# commit
```

set protocols dot1x filter sequence from source-address-ipv4

The **set protocols dot1x filter sequence from source-address-ipv4** command configures the source IPv4 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> sequence <*sequence-number*> **from source-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
source-address-ipv4 <*ipv4-address*>	Specifies the source IPv4 address of packets that match ACL rules. It must be an IPv4 subnet in address/prefix-length form. For example, 10.1.1.0/24.

Example

- Configure the source IPv4 address of packets that match ACL rules to 172.1.1.0/24.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from source-address-ipv4 172.1.1.0/24
admin@Xorplus# commit
```

set protocols dot1x filter sequence from source-address-ipv6

The **set protocols dot1x filter sequence from source-address-ipv6** command configures the source IPv6 address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from source-address-ipv6** <*ipv6-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
source-address-ipv6 <*ipv6-address*>	Specifies the source IPv6 address of packets that match ACL rules. It must be an IPv6 subnet in address/prefix-length form. For example, 0a::1/128.

Example

- Configure the source IPv6 address of packets that match ACL rules to 0a::1/128.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from source-address-ipv6 0a::1/128
admin@Xorplus# commit
```

set protocols dot1x filter sequence from source-port

The **set protocols dot1x filter sequence from source-port** command configures the source port information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from *source-port*** <*port-number*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
source-port <*port-number*>	Specifies the source port of packets that match ACL rules. The value is an integer. It could be a port number or a range of port number, i.e. 6000; 6000..7000, which indicates port range from 6000 to 7000.

Example

- Configure the source port of packets that match ACL rules to 7000.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from source-port 7000
admin@Xorplus# commit
```

set protocols dot1x filter sequence from protocol

The **set protocols dot1x filter sequence from protocol** command configures the protocol type information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> sequence <*sequence-number*> **from protocol [icmp | igmp | ip | ospf | others**<*protocol-number*> **| udp | tcp]**

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
protocol [icmp | igmp | ip | ospf | others <*protocol-number***> | udp | tcp]**	Specifies a protocol name or a protocol number. • Protocol name could be **icmp, igmp, ip, ospf, udp** or **tcp**. • Protocol number is an integer that ranges from 0 to 255. For example, 8 for EGP, 9 for IGP, 47 for GRE, 88 for EIGRP, 103 for PIM, and 112 for VRRP.

Example

- Configure the protocol type of packets that match ACL rules to ICMP.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from protocol icmp
admin@Xorplus# commit
```

set protocols dot1x filter sequence then action

The **set protocols dot1x filter sequence then action** command configures the action for packets that match the ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **then action** <**discard** | **forward**>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
action <**discard** | **forward**>	Specifies the action for packets that match the ACL rules. The value could be **discard** or **forward**. • **discard:** Discard packets that match all match conditions in the same sequence number. • **forward:** Forward packets that match all match conditions in the same sequence number.

Example

- Configure the action for packets that match the ACL rules to discard.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 then discard
admin@Xorplus# commit
```

run show dot1x all

The **run show dot1x all** command displays the NAC information.

Command Syntax

run show dot1x all

Parameter

None.

Example

- Run **run show dot1x all** command to view the NAC information.

```
admin@Xorplus# run show dot1x all
Global-Info:
--------------------------------------------------------------------------------
NAS-IP              :  10.10.1.1
Block-VLAN          :  2
Block-VLAN-IP       :  172.16.1.1/24
WEB-AUTH-MODE   :  Remote
Server-Fail-VLAN           :  100
--------------------------------------------------------------------------------
```

Table 1 Description of the **run show dot1x all** command output

Item	Description
NAS-IP	Indicates the NAS IP address which is set to the L3 VLAN interface IP connected to the RADIUS server.
Block-VLAN	Indicates the VLAN ID for block VLAN.
Block-VLAN-IP	Indicates the IP address of the L3 block VLAN interface.
WEB-AUTH-MODE	Indicates the Web authentication mode, the value is **Remote**.
Server-Fail-VLAN	Indicates the VLAN to which the user ports will be added to when all the configured RADIUS servers are unreachable.

run show dot1x interface

The **run show dot1x interface** command displays the configuration information and port status of NAC authentication function on the interface.

Command Syntax

run show dot1x interface [**gigabit-ethernet** <*interface-name*>]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Optional. Specifies the physical interface name.

Usage Guidelines

You can use this command to view the NAC authentication information of the client on all the interface enabled with NAC or on a specified interface. This command can also be used to view the dynamic ACL and downloadable ACL information.

Example

- Run **run show dot1x interface gigabit-ethernet** <*interface-name*> command to view the detailed NAC information on a specified interface.

```
admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/48
Interface ge-1/1/48:
============================================================
  Client MAC                : 00:00:00:11:11:11
  Status                    : authorized
  Success Auth Method       : MAB
  Last Success Time         : Sun Mar 20 21:08:11 2022
  Traffic Class             : Other
  Downloadable Filter Name  : pica-dacl-mab (active)
============================================================

admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/13
Interface ge-1/1/13:
============================================================
  Client MAC                : 08:9e:01:9e:cc:fe
  Status                    : authorized
  Success Auth Method       : MAB
  Dynamic VLAN ID           : 200 (active)
============================================================


admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/14
Interface ge-1/1/14:
============================================================
  Client MAC                : 00:00:00:22:55:56
  Status                    : authorized
  Success Auth Method       : MAB
  Dynamic VLAN ID           : 200 (active)
  Downloadable Filter Name  : f1
============================================================


admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/15
Interface ge-1/1/15:
============================================================
  Client MAC                : 00:00:00:22:55:56
  Status                    : authorized
  Success Auth Method       : MAB
```

```
  Dynamic VLAN ID           : 200 (active)
  Dynamic Filter Name       : f2(active)
============================================================
```

- Run **run show dot1x interface** command to view the brief NAC information on all the NAC enabled interfaces.

```
admin@Xorplus# run show dot1x interface
Interface  802.1x  MAC-RADIUS  WEB  HOST-MODE  CLIENT-MAC  CLIENT-STATUS
-------------------------------------------------------------------------------------------------------------------------
ge-1/1/1  disable   enable      disable   single(0)        00:11:22:33:44:55   unauthorized
ge-1/1/3  disable   enable      enable    multiple(1)
```

Table 1. Description of the run show dot1x interface command output

Item	Description
Client MAC	Indicates the MAC address of the clients connected to the interface.
Status	Indicates the authentication status of the client. The value could be **unauthorized** or **authorized**.
Success Auth Method	Indicates the authentication method used when the authentication status is authorized. The value could be **Dot1x** or **MAB**.
Redirect URL	Indicates the redirect URL delivered from the AAA server before Web authentication succeeds.
Dynamic VLAN ID	Indicates the dynamic VLAN ID delivered from the RADIUS authentication server. The active or inactive in parentheses indicates whether the dynamic VLAN is configured on the switch.
Downloadable Filter Name	Displays the downloadable filter name that is delivered to the client. Users can use command **run show dot1x downloadable filter** [*<filter-name>*] to display the details of downloadable filter rule.
Dynamic Filter Name	Displays the dynamic filter name that is delivered to the client. The active or inactive in parentheses indicates whether the dynamic filter is configured on the switch.
Interface	Indicates the physical interfaces enabled NAC.
802.1x	Indicates whether the 802.1X authentication is enabled. • **enable**: indicates the 802.1X authentication is enabled. • **disable**: indicates the 802.1X authentication is disabled.
MAC-RADIUS	Indicates whether the MAB authentication is enabled. • **enable**: indicates the MAB authentication is enabled. • **disable**: indicates the MAB authentication is disabled.
WEB	Indicates whether the Web authentication is enabled. • **enable**: indicates the Web authentication is enabled. • **disable**: indicates the Web authentication is disabled.
HOST-MODE	Host mode of interface and the number of active sessions. The value could be **single(N)** or **multiple(N)**, where "N" is the number of active sessions. • **single(N):** Only one user is allowed to access the switch port, unless the user goes offline other users can try to access the port. The authentication will be restarted if port is bounced or client is changed. • **multiple(N):** Multiple clients connect to the network through the same switch port. If a user goes offline, the network access rights of other users are not affected. At most 8 clients are allowed to be authenticated on a single switch port, the ninth will be added into the pending list. The default host mode is **single**. Note that changing host mode from CLI will cause re-authentication for all online users of the port.
CLIENT-MAC	Indicates the MAC address of the clients connected to the interface.
CLIENT-STATUS	Indicates the authentication status of the client. The value could be **unauthorized** or **authorized**.

run show dot1x server

The **run show dot1x server** command displays the reachability of the AAA servers configured on the switch.

Command Syntax

run show dot1x server

Parameter

None.

Example

- Run **run show dot1x server** command to view reachability of the RADIUS servers.

```
admin@Xorplus# run show dot1x server
Server-IP         Status        Priority  Retry-Interval  Retry-Num  Detect-Interval   Consecutive-Detect-Num
---------------   ------------  --------  --------------  ---------  --------------    ----------------------
10.10.53.72       reachable     ...       5   Sec(s)      5          5   Sec(s)        8
```

Table 1. Description of the run show dot1x server command output

Item	Description
Server-IP	Indicates the RADIUS Server IP configured on the switch.
Status	Indicates whether the RADIUS server is reachable. The value could be **active**, **reachable** or **unreachable**. If the server is reachable and currently selected for NAC authentication, the “Status” of this server is **active**.
Priority	Indicates the priority of AAA server. The value is an integer that ranges from 1 to 3. Priority of 1 is higher than 3. “...” indicates a lowest priority if not configured for the AAA server. Note: The AAA servers are listed in the order of priority.
Retry-Interval	Indicates the interval for re-sending the authentication messages to the AAA server when the AAA server does not respond during NAC authentication.
Retry-Num	Indicates the maximum number of authentication attempts when the AAA server does not respond during NAC authentication.
Detect-Interval	Indicates the interval at which the switch sends Test Radius Request detection message to the AAA server to detect the server reachability.
Consecutive-Detect-Num	Indicates the number of Test Radius Request messages that the switch consecutively sends to the AAA server to detect the server reachability.

run show dot1x dynamic filter

The **run show dot1x dynamic filter** command displays the dynamic filter rules configured on the switch.

Command Syntax

run show dot1x dynamic filter *<filter-name>*

Parameter

Parameter	Description
<filter-name>	Optional. Specifies the dynamic ACL filter name. The value is a string. • If displaying with a filter name, display the specified dynamic ACL filter rules. • If displaying without a filter name, display all the configured dynamic ACL filter rules.

Exampe

- Configure the dynamic ACL rules on the switch then run **run show dot1x dynamic filter** command to view the configurations.

```
admin@Xorplus# set protocols dot1x filter f4 sequence 500 from destination-address-ipv4 192.168.2.0/24
admin@Xorplus# set protocols dot1x filter f4 sequence 500 then forward
admin@Xorplus# run show dot1x dynamic filter
==========================================================================
Filter: f4
    Description :
    --------------------------------------------------------------------
    Sequence            : 500
        Description      :
        Match counter    :  60544 packets
        Match Condition  :
                          Destination IPv4Net : 192.168.2.0/24
        Action           : FORWARD
==========================================================================
        Applied Clients   : ge-1/1/1 00:00:00:11:22:33
```

run show dot1x downloadable filter

The **run show dot1x downloadable filter** command displays the downloadable filter rules delivered from the RADIUS authentication server.

Command Syntax

run show dot1x downloadable filter [<*filter-name*>]

Parameter

Parameter	Description
<*filter-name*>	Optional. Specifies the downloadable filter rule name.

Exampe

- Display the downloadable filter rules delivered from the RADIUS authentication server.

```
admin@Xorplus# run show dot1x downloadable filter
================================================
Filter: IP_Attendance_CTRL_Access
Description     :
------------------------------------------------------------------------
Sequence        : 1
Description     :
Match counter   : 0 packets
Match Condition : L4 Destination Port  : 67..67
                  L4 Source Port       : 68..68
                  Protocol             : udp
                  Action               : Forward
 ------------------------------------------------------------------------
Sequence        : 2
Description     :
Match counter   : 51 packets
Match Condition : L4 Destination Port  : 53..53
                  Protocol             : udp
                  Action               : Forward
------------------------------------------------------------------------
```

run show dot1x interface statistics gigabit-ethernet

The **run show dot1x interface statistics gigabit-ethernet** command displays the 802.1X statistics information on an interface.

Command Syntax

run show dot1x interface statistics gigabit-ethernet <*interface-name*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. The value is a string.

Example

- Run **run show dot1x interface statistics gigabit-ethernet** command to display the 802.1X statistics information on interface ge-1/1/1.

```
admin@Xorplus# run show dot1x interface statistics gigabit-ethernet ge-1/1/1
Interface ge-1/1/1:
================================================================================
    Client MAC : 00:11:22:33:44:55
    ----------------------------------------------------------------------
    SENT:
      EAPOL LogOff Packets : 0
      EAPOL EAP Packets    : 0
      EAP Request Packets  : 0
      EAP Response Packets : 0
      EAP Success Packets  : 0
      EAP Failure Packets  : 0
      Radius Packets       : 2
    ----------------------------------------------------------------------
    RECEIVED:
      EAPOL Start Packets  : 0
      EAPOL LogOff Packets : 0
      EAPOL EAP Packets    : 0
      EAP Request Packets  : 0
      EAP Response Packets : 0
      EAP Success Packets  : 0
      EAP Failure Packets  : 0
      Radius Packets       : 1
```

set protocols dot1x server-fail recovery-method

The **set protocols dot1x server-fail recovery-method** command configures the way to get the client port out the server fail VLAN when the server is reachable.

Command Syntax

set protocols dot1x server-fail recovery-method <auto | manual | timer >

Parameter

Parameter	Description
recovery-method <auto | manual | timer >	Specifies the way to get the client port out the server fail VLAN when the server is reachable, the value could be **auto**, **manual** or **timer**. • **auto**: The system automatically removes the client port from the server fail VLAN when the server is reachable, and take authentication again. • **manual**: Manually remove the client port from the server fail VLAN when the server is reachable. Users need to clear MAC or bounce port to trigger client to take authentication again, otherwise the client port will not be removed from the server fail VLAN when the server is reachable. • **timer**: Remove the client port from the server fail VLAN after a certain amount of time when the server is reachable. The timer can be set by command **set protocols dot1x interface recovery-timeout**. The default value is **manual**.

Usage Guidelines

If all the RADIUS servers are unreachable, the port connected to the client will be added to the server fail VLAN, and the packets from the client can be forwarded in server fail VLAN. The switch continues to send the detection packets continuously until the server is reachable. If one of the RADIUS servers is reachable, the switch removes this client from the server fail VLAN and adds it back into the block VLAN. This command configures the way to get the client port out the server fail VLAN when the server is reachable.

Example

- Configure the way to get the client port out the server fail VLAN when the server is reachable.

```
admin@Xorplus# set protocols dot1x server-fail recovery-method auto
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip consecutive-detect-num

The **set protocols dot1x aaa radius authentication server-ip consecutive-detect-num** command configures the number of Test Radius Request messages that the switch consecutively sends to the AAA server to detect the server reachability.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <ipv4-address> **consecutive-detect-num** <*detect-num*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of AAA server.
consecutive-detect-num <*detect-num*>	Specifies the number of Test Radius Request message that the switch consecutively sends to the server. The value is an integer that ranges from 1 to 10. The default value is 3.

Usage Guidelines

The AAA server is considered to be reachable only when every Test Radius Request message consecutively sent by the switch receives a RADIUS access-accept message reply from the AAA server, otherwise the server is considered unreachable. The switch will continue to send the Test Radius Request message until the server is reachable.

Example

- Configure the number of Test Radius Request messages that the switch consecutively sends.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 consecutive-detect-num 5
admin@Xorplus# commit
```

set protocols dot1x aaa vrf mgmt-vrf

The **set protocols dot1x aaa vrf mgmt-vrf** command configures to run the 802.1X protocols in the management VRF.

Command Syntax

set protocols dot1x aaa vrf mgmt-vrf

Parameter

None.

Usage Guidelines

802.1X protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding AAA server is required to be route reachable in the VRF running 802.1X protocol.

Using this command to modify the VRF where to run the 802.1X service does not affect users who are currently authenticated successfully and online, it will only affect users who need to do DOT1X authentication later.

Note: The latest configuration overrides the previous one.

Example

- Configure the 802.1X protocols to run in the management VRF.

```
admin@Xorplus# set protocols dot1x aaa vrf mgmt-vrf
admin@Xorplus# commit
```

set protocols dot1x interface session-timeout

The **set protocols dot1x interface session-timeout** command configures the expire timer for the authenticated session.

Command Syntax

set protocols dot1x [**interface** <*interface-name*>] **session-timeout** <*session-timeout*>

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on. If no interface is specified, it represents a global configuration.
session-timeout <*session-timeout*>	Specifies the expire timer for the authenticated session. The value is an integer that ranges from 0 to 86400, in seconds. The default value is 3600s. Note that, “0” indicates authenticated session will never expire.

Usage Guidelines

The authenticated session will expire after a period of **session-timeout** and start a new authentication process. The switch will send request packet to the AAA server or the client after the expire timer for re-authentication.

The AAA server can also issue session-timeout, which takes precedence over the local configuration on the switch. About the processing for session-timeout Attribute issued by the AAA server, see section **Response to session-timeout Attribute** in Principle of NAC.

Note:

- The session timeout configuration based on an interface takes precedence over that of the global configuration.
- Configuration changes will only affect clients who need to do DOT1X authentication later.

Example

- Configure the global session expire timer for the authenticated session.

```
admin@Xorplus# set protocols dot1x session-timeout 1800
admin@Xorplus# commit
```

set protocols dot1x interface recovery-timeout

The **set protocols dot1x interface recovery-timeout** command configures the timer after which to remove the client port from the server fail VLAN when the server is reachable.

NOTE: The **recovery-timeout** takes effect only when the recovery-method is set to “timer”.

Command Syntax

set protocols dot1x interface *<interface-name>* **recovery-timeout** *<recovery-timeout>*

Parameter

Parameter	Description
interface *<interface-name>*	Optional. Specifies the physical interface name. The value could be ge-1/1/1, xe-1/1/2, and so on.
recovery-timeout *<recovery-timeout>*	Specifies the timer after which to remove the client port from the server fail VLAN when the server is reachable. The value is an integer that ranges from 300 to 86400, in seconds. The default value is 3600 seconds.

Usage Guidelines

This command is a interface-based configuration. PICOS supports to configure the timer globally for all the switch interface after which to remove the client port from the server fail VLAN when the server is reachable by using the command set protocols dot1x server-fail recovery-timeout.

Note that the recovery timeout configuration based on an interface takes precedence over that of the global configuration.

Example

- Configure the timer after which to remove the client port from the server fail VLAN when the server is reachable.

```
admin@Xorplus# set protocols dot1x recovery-timeout 1800
admin@Xorplus# commit
```

set protocols dot1x server-fail recovery-timeout

The **set protocols dot1x server-fail recovery-timeout** command configures the timer globally after which to remove the client port from the server fail VLAN when the server is reachable.

NOTE: The **recovery-timeout** takes effect only when the recovery-method is set to “timer”.

Command Syntax

set protocols dot1x server-fail recovery-timeout <*recovery-timeout*>

Parameter

Parameter	Description
recovery-timeout <*recovery-timeout*>	Specifies the timer after which to remove the client port from the server fail VLAN when the server is reachable. The value is an integer that ranges from 300 to 86400, in seconds. The default value is 3600 seconds.

Usage Guidelines

This command is a global configuration for all the switch interface. PICOS supports to configure the timer based on an interface after which to remove the client port from the server fail VLAN when the server is reachable by using the command set protocols dot1x interface recovery-timeout.

Note that the recovery timeout configuration based on an interface takes precedence over that of the global configuration.

Example

- Configure the timer after which to remove the client port from the server fail VLAN when the server is reachable.

```
admin@Xorplus# set protocols dot1x recovery-timeout 1800
admin@Xorplus# commit
```

set protocols dot1x interface max-sessions

The **set protocols dot1x interface max-sessions** command configures the maximum number of NAC sessions that are allowed to be established on a specified interface.

Command Syntax

set protocols dot1x interface <*interface-name*> **max-sessions** <*max-sessions-number*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a physical interface name. The value is like ge-1/1/1, te-1/1/3, etc.
max-sessions <*max-sessions-number*>	Specifies the maximum number of NAC sessions. The value is an integer in the range of 0 to 512. The default value is 0, indicating that there is no limit on the number of NAC sessions.

Usage Guidelines

This command is configured on a specified interface. Users can also configure the maximum number of NAC sessions globally by using the command **set protocols dot1x max-sessions-per-port** <*max-sessions-number*>.

The maximum number of NAC sessions configured on an interface has a higher priority over the value configured globally.

Example

- Configure the maximum number of NAC sessions that are allowed to be established on interface ge-1/1/1 to 30.

```
admin@Xorplus# set protocols dot1x interface ge-1/1/1 max-sessions 30
admin@Xorplus# commit
```

set protocols dot1x max-sessions-per-port

The **set protocols dot1x max-sessions-per-port** command globally configures the maximum number of NAC sessions that are allowed to be established on each port enabled for NAC.

Command Syntax

set protocols dot1x max-sessions-per-port <*max-sessions-number*>

Parameter

Parameter	Description
max-sessions-per-port <*max-sessions-number*>	Specifies the maximum number of NAC sessions. The value is an integer in the range of 0 to 512. The default value is 0, indicating that there is no limit on the number of NAC sessions.

Usage Guidelines

The command **set protocols dot1x max-sessions-per-port** <*max-sessions-number*> is a global setting, which will take effect on all the interfaces enabled for NAC.

PicOS also provides the command **set protocols dot1x max-sessions-per-port** <*max-sessions-number*> to configure the maximum number of NAC sessions that are allowed to be established on a specified interface.

The maximum number of NAC sessions configured on an interface has a higher priority over the value configured globally.

Example

- Configure the maximum number of NAC sessions that are allowed to be established on each interface enabled for NAC globally.

```
admin@Xorplus# set protocols dot1x max-sessions-per-port 30
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip auth-port

The **set protocols dot1x aaa radius authentication server-ip auth-port** command configures the UDP port of the RADIUS server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **auth-port** <*port-number*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
auth-port <*port-number*>	Specifies UDP port of RADIUS authentication server. The value is an integer that ranges from 1 to 65535. The default value is 1812.

Example

- Configure the UDP port of the RADIUS authentication server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 auth-port 5100
admin@Xorplus# commit
```

set protocols dot1x aaa radius authentication server-ip acct-port

The **set protocols dot1x aaa radius authentication server-ip acct-port** command configures the UDP port of the RADIUS accounting server.

Command Syntax

set protocols dot1x aaa radius authentication server-ip <*ipv4-address*> **acct-port** <*port-number*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies IPv4 address of RADIUS authentication server.
acct-port <*port-number*>	Specifies UDP port of RADIUS accounting server. The value is an integer that ranges from 1 to 65535. The default value is 1813.

Example

- Configure the UDP port of the RADIUS accounting server.

```
admin@Xorplus# set protocols dot1x aaa radius authentication server-ip 10.10.10.1 acct-port 5200
admin@Xorplus# commit
```

set protocols dot1x aaa radius dynamic-author client port

The **set protocols dot1x aaa radius dynamic-author client port** command configures the UDP port of the RADIUS dynamic authorization server for CoA function. This is the UDP port on the switch side.

Command Syntax

set protocols dot1x aaa radius dynamic-author client <*ip-address*> **port** <*port-number*>

Parameter

Parameter	Description
client <*ip-address*>	Specifies IPv4 address of the RADIUS dynamic authorization client. This is the IP address of the RADIUS server.
port <*port-number*>	Specifies UDP port of RADIUS dynamic authorization server. The value is an integer that ranges from 1 to 65535. The default value is 3799.

Example

- Configure the UDP port of the RADIUS dynamic authorization server.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 192.16.10.1 port 8888
admin@Xorplus# commit
```

run show dot1x radius-port

The **run show dot1x radius-port** command shows the UDP port information of 802.1X RADIUS server and dynamic authorization server for CoA.

Command Syntax

run show dot1x radius-port

Parameter

None.

Example

- View the UDP port information of 802.1X RADIUS server and dynamic authorization server for CoA.

```
admin@Xorplus# run show dot1x radius-port
Server-IP          Authentication     Accounting        CoA
---------------  ----------------    ----------------  ----------------
2.2.2.2            N/A                N/A               9999
5.5.5.5            N/A                N/A               3799
1.1.1.1            2222               1111              8888
3.3.3.3            6666               7777              N/A
4.4.4.4            1812               1813              N/A
```

NOTEs:

- “N/A” indicates related RADIUS service is not available. For example, in above show result, 2.2.2.2 and 5.5.5.5 are dynamic authorization clients for CoA only, and 4.4.4.4 is a RADIUS server for authentication and accounting without CoA.

  The UDP port number of 802.1X RADIUS server shows “N/A” if no RADIUS authentication server IP is configured. The UDP port number of dynamic authorization server of CoA shows “N/A” if no RADIUS dynamic authorization client IP is configured.

- The IP addresses of RADIUS dynamic authorization client are shown in the column “Server-IP”, as they are usually located on the RADIUS server.

set protocols dot1x filter sequence from destination-mac-address

NOTE:
This command is no longer supported from version 4.3.2, since this filter has been deprecated.

The **set protocols dot1x filter sequence from destination-mac-address** command configures the destination MAC address information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> **sequence** <*sequence-number*> **from destination-mac-address** <*mac-address*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
destination-mac-address <*mac-address*>	Specifies the destination MAC address of packets that match ACL rules. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Example

- Configure the destination MAC address of packets that match ACL rules to 10:50:ba:27:be:d2.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from destination-mac-address 10:50:ba:27:be:d2
admin@Xorplus# commit
```

set protocols dot1x filter sequence from vlan

NOTE:
This command is no longer supported from version 4.3.2, since this filter has been deprecated.

The **set protocols dot1x filter sequence from vlan** command configures the VLAN ID information of the matching packets based on the NAC-based ACL rules.

Command Syntax

set protocols dot1x filter <*filter-name*> sequence <*sequence-number*> **from vlan** <*vlan-id*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the ACL filter name. The value is a string.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Configure the VLAN ID of packets that match ACL rules to 100.

```
admin@Xorplus# set protocols dot1x filter f1 sequence 2 from vlan 100
admin@Xorplus# commit
```

SNMP Configuration Commands

- set protocols snmp trap-group targets security-name
- set protocols lldp snmp-trap
- set protocols snmp trap-group event cpu-threshold enable
- set protocols snmp trap-group event cpu-threshold high
- set protocols snmp trap-group event cpu-threshold interval
- set protocols snmp trap-group event cpu-threshold low
- set protocols snmp trap-group event mac-threshold enable
- set protocols snmp trap-group event mac-threshold interval
- set protocols snmp trap-group event mac-threshold limit
- set protocols snmp trap-group vrf mgmt-vrf
- set protocols snmp trap-group version
- set protocols snmp v3 enable
- set protocols snmp v3 usm-user
- set protocols snmp v3 usm-user group
- set protocols snmp v3 group notify-view
- set protocols snmp v3 group read-view
- set protocols snmp v3 group write-view
- set protocols snmp v3 group security-level
- set protocols snmp v3 usm-user authentication-mode
- set protocols snmp v3 usm-user authentication-key
- set protocols snmp v3 usm-user privacy-mode
- set protocols snmp v3 usm-user privacy-key
- set protocols snmp v3 mib-view subtree mask
- set protocols snmp v3 mib-view subtree type
- set protocols snmp trap-group source-interface
- set protocols snmp community
- set protocols snmp community authorization
- set protocols snmp community clients
- set protocols snmp contact
- set protocols snmp location
- run show snmp statistics

set protocols snmp trap-group targets security-name

The **set protocols snmp trap-group targets security-name** command configures NMS for receiving the trap messages.

> ⚠ Please note trap-messages can be actually sent out only if the concerning user, group and notify-view have been configured.

Command Syntax
set protocols snmp trap-group targets *<IPv4_address>* **security-name** <security-name>
delete protocols snmp trap-group targets *<IPv4_address>*

Parameter

Parameter	Description
targets *<IPv4_address>*	Specifies the address of the target host that receives SNMP traps. **NOTE:** The IP address specified by address and the security name specified by securityname together identify a target host.
security-name <security-name>	Specifies the user security name displayed on the NMS. For SNMPv3, **security name** must be configured as the user name. **security name** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **security name** configured. **security name** is used to distinguish multiple hosts that generate trap messages.

Example

•This example configures a NMS for receiving the trap messages.

```
admin@XorPlus# set protocols snmp trap-group targets 10.10.51.42 security-name user1
admin@XorPlus# commit
```

set protocols lldp snmp-trap

The **set protocols lldp snmp-trap** command is used to enable or disable the SNMP trap for LLDP function.

Command Syntax

set protocols lldp snmp-trap <**true** | **false**>

Parameter

Parameter	Description
snmp-trap <**true** | **false**>	Enable or disable the SNMP trap for LLDP function. The value could be **true** or **false**. • **true**: Enable the SNMP trap for LLDP function, the system can send LLDP trap message to NMS. • **false**: Disable the SNMP trap for LLDP function, then there will be no more LLDP trap message sends to NMS. The default value is **true**.

Example

- Disable the SNMP trap for LLDP function.

```
admin@Xorplus# set protocols lldp snmp-trap false
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold enable

The **set protocols snmp trap-group event cpu-threshold enable** command is used to enable or disable the function of monitoring the switch CPU usage and sending an SNMP Trap message when the switch CPU usage exceeds the overload threshold or falls below the low threshold.

Command Syntax

set protocols snmp trap-group event cpu-threshold enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enable or disable the function of monitoring the switch CPU usage and sending an SNMP Trap message. The value could be **true** or **false**. • **true**: enables the function of monitoring the switch CPU usage and sending an SNMP Trap message. • **false**: disables the function of monitoring the switch CPU usage and sending an SNMP Trap message. The function is **disabled** by default.

Usage Guidelines

After this function is enabled, the device can generate an SNMP Trap alarm message when the switch CPU usage exceeds the overload threshold or falls below the low threshold, so you can effectively monitor CPU usage and optimize system performance to maintain data forwarding and network topology stability.

Example

- Enable the function of monitoring the switch CPU usage and sending an SNMP Trap message.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold enable true
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold high

The **set protocols snmp trap-group event cpu-threshold high** command sets the overload threshold for CPU usage monitoring to send SNMP Trap messages.

Command Syntax

set protocols snmp trap-group event cpu-threshold high <*high-value*>

Parameter

Parameter	Description
high <*high-value*>	Specifies the overload threshold for CPU usage monitoring to send SNMP Trap messages. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 80.

Usage Guidelines

Use this command to set the CPU usage overload threshold. When CPU usage exceeds the overload threshold for a continuous time period, the system logs the event and sends an SNMP Trap message. By viewing log information, you can effectively monitor CPU usage.

NOTE:

- If the CPU usage reaches 100%, the system won't send SNMP Trap message.
- Please set the CPU usage monitoring overload threshold carefully. If the CPU usage overload threshold is set too small, the system generates alarms frequently. If the CPU usage overload threshold is set too large, you cannot be notified of the CPU usage overload in a timely manner.

Example

- Set the overload threshold for CPU usage to 80%.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold high 80
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold interval

The **set protocols snmp trap-group event cpu-threshold interval** command configures the time duration for which the CPU usage continues to exceed the overload threshold or fall below the low threshold.

Command Syntax

set protocols snmp trap-group event cpu-threshold interval <*interval*>

Parameter

Parameter	Description
interval <*interval*>	Specifies the time duration. The value is an integer, in seconds, that ranges from 5 to 4294967295. The default value is 300s.

Usage Guidelines

Generally, if the CPU usage of the system exceeds the threshold for a short period of time, the CPU usage is considered to be in the normal range, and no CPU usage alarm will be generated. Similarly, if the CPU usage falls below the low threshold but doesn't persist for the duration of **interval** time, again, no CPU usage alarm will be sent.

The system samples CPU usage one time every 5 seconds, if the CPU usage is out of the threshold range over this interval time, a SNMP trap message will be sent. But once CPU usage falls back into the threshold range and the duration time is not up, the duration time then will be recalculated and the trap message won't be sent.

Example

- Configure the time duration when the CPU usage continues to exceed the overload threshold or fall below the low threshold to 300s.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold interval 300
admin@Xorplus# commit
```

set protocols snmp trap-group event cpu-threshold low

The **set protocols snmp trap-group event cpu-threshold low** command configures sets the low threshold for CPU usage monitoring to send SNMP Trap messages.

Command Syntax

set protocols snmp trap-group event cpu-threshold low <*low-value*>

Parameter

Parameter	Description
low <*low-value*>	Specifies the low threshold for CPU usage monitoring. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 20.

Usage Guidelines

When CPU usage falls below the low threshold for a continuous time period, the system logs the event and sends an SNMP Trap message. By viewing log information, you can effectively monitor CPU usage.

Example

- Set the low threshold for CPU usage to 20%.

```
admin@Xorplus# set protocols snmp trap-group event cpu-threshold low 20
admin@Xorplus# commit
```

set protocols snmp trap-group event mac-threshold enable

The **set protocols snmp trap-group event mac-threshold enable** command is used to enable or disable the function of monitoring the switch MAC address table usage and sending an SNMP Trap message when the switch MAC address table usage exceeds the limit threshold.

Command Syntax

set protocols snmp trap-group event mac-threshold enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enable or disable the function of monitoring the switch MAC address table usage and sending an SNMP Trap message. The value could be **true** or **false**. **true**: enables the function of monitoring the switch MAC address table usage and sending an SNMP Trap message. **false**: disables the function of monitoring the switch MAC address table usage and sending an SNMP Trap message. The function is **disabled** by default.

Usage Guidelines

After this function is enabled, the device can generate an SNMP Trap alarm message when the switch MAC address table usage exceeds the limit threshold, you can effectively monitor MAC address table usage and optimize system performance to maintain data forwarding and network topology stability.

Example

- Enable the function of monitoring the switch MAC address table usage and sending an SNMP Trap message.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold enable true
admin@Xorplus# commit
```

set protocols snmp trap-group event mac-threshold interval

The **set protocols snmp trap-group event mac-threshold interval** command configures the time duration when the MAC address table usage continues to exceed the limit threshold.

Command Syntax

set protocols snmp trap-group event mac-threshold interval <*interval*>

Parameter

Parameter	Description
interval <*interval*>	Specifies the time duration. The value is an integer, in minutes, that ranges from 5 to 4294967295. The default value is 15 minutes.

Usage Guidelines

The system samples MAC address table usage one time every 10 seconds, if the MAC address table usage exceed the limit threshold over this interval time, a SNMP trap message will be sent. But once MAC address table usage falls back below the threshold when the duration time is not up, the duration time then will be recalculated and the trap message won't be sent.

Example

- Configure the time duration when the MAC address table usage continues to exceed the limit threshold to 50 minutes.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold interval 50
admin@Xorplus# commit
```

set protocols snmp trap-group event mac-threshold limit

The **set protocols snmp trap-group event mac-threshold limit** command sets the limit threshold for MAC address table usage monitoring to send SNMP Trap messages.

Command Syntax

set protocols snmp trap-group event mac-threshold limit <*limit-value*>

Parameter

Parameter	Description
limit <*limit-value*>	Specifies the limit threshold for MAC address table usage monitoring to send SNMP Trap messages. The value is an integer that ranges from 1 to 100, indicating 1% to 100%. The default value is 50.

Usage Guidelines

Use this command to set the MAC address table usage limit threshold. When MAC address table usage exceeds the limit threshold over a continuous period of time, the system logs the event and sends an SNMP Trap message. By viewing log information, you can learn about MAC address table usage.

NOTE:

Please set the MAC address table usage monitoring limit threshold carefully. If the MAC address table usage limit threshold is set too small, the system generates alarms frequently. If the MAC address table usage limit threshold is set too large, you cannot get MAC address table usage overload immediately.

Example

- Set the limit threshold for MAC address table usage monitoring to 50%.

```
admin@Xorplus# set protocols snmp trap-group event mac-threshold limit 50
admin@Xorplus# commit
```

set protocols snmp trap-group vrf mgmt-vrf

The **set protocols snmp trap-group vrf mgmt-vrf** command configures to run the SNMP Trap service in the management VRF.

Command Syntax

set protocols snmp trap-group vrf mgmt-vrf

Parameter

None.

Usage Guidelines

SNMP Trap management service runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding Network Management System (NMS) is required to be route reachable in the VRF running SNMP Trap management service.

Note: The latest configuration overrides the previous one.

Example

- Configure the SNMP Trap service to run in the management VRF.

```
admin@Xorplus# set protocols snmp trap-group vrf mgmt-vrf
admin@Xorplus# commit
```

set protocols snmp trap-group version

The **set protocols snmp trap-group version** command configures the version of the SNMP trap messages.The default version is v2.

Command Syntax
set protocols snmp trap-group version <*version*>
delete protocols snmp trap-group version <*version*>

Parameter

- <version> version of the trap messages
  - **v1** version 1
  - **v2** version 2
  - **v3** version 3

Example

- This example configures version 3 to the trap messages

```
admin@XorPlus# set protocols snmp trap-group version v3
admin@XorPlus# commit
```

set protocols snmp v3 enable

The **set protocols snmp v3 enable** command can be used to enable or disable SNMPv3. The default version of the SNMP is v2.

Command Syntax
set protocols snmp v3 enable *<boolean>*

Parameter

Parameter	Description
enable *<boolean>*	Enable or disable SNMPv3. The value could be **true** or **false**. • **true**: enables SNMPv3. • **false**: disables SNMPv3. The default version of the SNMP is v2.

Example

•This example enables SNMPv3.

```
admin@XorPlus# set protocols snmp v3 enable true
admin@XorPlus# commit
```

set protocols snmp v3 usm-user

The **set protocols snmp v3 usm-user** command configures an SNMP user name.

> ⚠ A user without adding to any groups only can be read all the OIDs by NMS (could not be written or send trap-messages).

Command Syntax
set protocols snmp v3 usm-user <*user-name*>

delete protocols snmp v3 usm-user <*user-name*>

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.

Example

•This example configures a user user1 without adding to any groups.

```
admin@XorPlus# set protocols snmp v3 usm-user user1
admin@XorPlus# commit
```

set protocols snmp v3 usm-user group

> If you add a user to an SNMP group, you have to configure the read-view, write-view or notify-view for the group. Or NMS will have no authority (writing, reading, being notified) operated on the user.

The **set protocols snmp v3 usm-user group** command adds a user to an SNMP group.

Command Syntax
set protocols snmp v3 usm-user <*user-name*> **group** <*group-name*>

delete protocols snmp v3 usm-user <*user-name*> **group**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
group <*group-name*>	Specifies the name of the group to which a user belongs. The value is a string.

Example

•This example adds user1 to SNMP group1.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 group group1
admin@XorPlus# commit
```

set protocols snmp v3 group notify-view

The **set protocols snmp v3 group notify-view** command configures a notify view for an SNMP group.

> ⚠ Some OIDs which are capable of sending trap-messages can be added to the notify-view optionally. If not doing so, the user will not send trap-messages initiatively.

Command Syntax
set protocols snmp v3 group <*group-name*> **notify-view** <*view-name*>

delete protocols snmp v3 group <*group-name*> **notify-view**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
notify-view <*view-name*>	Specifies a notify view. The value is a string.

Example

•This example configures a notify view name for a group.

```
admin@XorPlus# set protocols snmp v3 group group1 notify-view view1
admin@XorPlus# commit
```

set protocols snmp v3 group read-view

The **set protocols snmp v3 group read-view** command configures a read-only view for an SNMP group.

> A user in the group which is configured with read-view only can be read by NMS while cannot be written or send trap-messages. Writing and notifying authority can be gained by NMS only after you configure the corresponding view.

Command Syntax
set protocols snmp v3 group <*group-name*> **read-view** <*view-name*>

delete protocols snmp v3 group <*group-name*> **read-view**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
read-view <*view-name*>	Specifies a read-only view. The value is a string.

Example

•This example configures a read-view name for a group.

```
admin@XorPlus# set protocols snmp v3 group group1 read-view view1
admin@XorPlus# commit
```

set protocols snmp v3 group write-view

The **set protocols snmp v3 group write-view** command configures a read-write view for an SNMP group.

> A user in the group which is configured with write-view only can be written by NMS while cannot send trap-messages initiatively. Notify authority can be gained when you configure the corresponding view.

Command Syntax
set protocols snmp v3 group <*group-name*> **write-view** <*view-name*>

delete protocols snmp v3 group <*group-name*> **write-view**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
write-view <*view-name*>	Specifies a read-write view. The value is a string.

Example

•This example configures a write-view name for a group.

```
admin@XorPlus# set protocols snmp v3 group group1 write-view view1
admin@XorPlus# commit
```

set protocols snmp v3 group security-level

The **set protocols snmp v3 group security-level** command configure the security level of an SNMP group.

> ⚠ When the security-level of a group is AuthNoPriv or AuthPriv,the user in that group should be configured with Authentication-mode, Authentication-key even as well as privacy-mode and privacy-key.

Command Syntax

set protocols snmp v3 group <*group-name*> **security-level** <**AuthNoPriv | AuthPriv | NoAuthNoPriv**>

delete protocols snmp v3 group <*group-name*> **security-level**

Parameter

Parameter	Description
group <*group-name*>	Specifies the name of an SNMP group. The value is a string.
security-level <**AuthNoPriv	AuthPriv	NoAuthNoPriv**>	Specifies the security level of the SNMP group. The value could be **AuthNoPriv**, **AuthPriv** or **NoAuthNoPriv.** • **AuthNoPriv**: authenticates SNMP messages without encryption. • **AuthPriv**: authenticates and encrypts SNMP messages. • **NoAuthNoPriv**: does not authenticate or encrypt SNMP messages.

Example

•This example configures group1 to AuthPriv.

```
admin@XorPlus# set protocols snmp v3 group group1 security-level AuthPriv
admin@XorPlus# commit
```

set protocols snmp v3 usm-user authentication-mode

The **set protocols snmp v3 usm-user authentication-mode** command configures authentication-mode for a user. If authentication-mode is configured, authentication-key also needs to be configured.

Command Syntax

set protocols snmp v3 usm-user <*user-name*> **authentication-mode** <**md5 | none | sha**>

delete protocols snmp v3 usm-user <*user-name*> **authentication-mode**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
authentication-mode <**md5	none	sha**>	Specifies the authentication-mode for a user. The value could be **md5**, **none** or **sha**. • **md5**: Specifies HMAC-MD5-96 as the authentication protocol. • **none**: Do not authenticate the user. • **sha**: Specifies HMAC-SHA-96 as the authentication protocol.

Example

•This example configures md5 authentication mode for user1.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 authentication-mode md5
admin@XorPlus# commit
```

set protocols snmp v3 usm-user authentication-key

The **set protocols snmp v3 usm-user authentication-key** command configures a authentication key for a user.

Command Syntax
set protocols snmp v3 usm-user <*user-name*> **authentication-key** <*authentication-key*>

delete protocols snmp v3 usm-user <*user-name*> **authentication-key**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
authentication-key <*authentication-key*>	Specifies the authentication key for a user. The value is a string that should be no less than 8 characters.

Example

•This example configures a authentication-key for a user.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 authentication-key u1111key
admin@XorPlus# commit
```

set protocols snmp v3 usm-user privacy-mode

The **set protocols snmp v3 usm-user privacy-mode** command configures privacy-mode for a uese. If you have configured privacy-mode for a user, privacy-key also needs to be configured.

Command Syntax

set protocols snmp v3 usm-user <*user-name*> **privacy-mode** <*privacy-mode* >

delete protocols snmp v3 usm-user <*user-name*> **privacy-mode**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
privacy-mode <*privacy-mode* >	Specifies the encryption protocol for a user. The value could be **3des**, **aes128**, **des** or **none**.

Example

•This example configures **des** for user1.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 privacy-mode des
admin@XorPlus# commit
```

set protocols snmp v3 usm-user privacy-key

The **set protocols snmp v3 usm-user privacy-key** command configures a privacy key for a user.

Command Syntax
set protocols snmp v3 usm-user <*user-name*> **privacy-key** <*privacy-key*>

delete protocols snmp v3 usm-user <*user-name*> **privacy-key**

Parameter

Parameter	Description
usm-user <*user-name*>	Specifies the name of a user. The value is a string.
privacy-key <*privacy-key*>	Specifies the privacy key for a user. The value is a string that should be no less than 8 characters.

Example

•This example configures a privacy-key for a user.

```
admin@XorPlus# set protocols snmp v3 usm-user user1 privacy-key u1111key
admin@XorPlus# commit
```

set protocols snmp v3 mib-view subtree mask

The **set protocols snmp v3 mib-view subtree mask** command configures a MIB view which is used as a view of a group. And users can just set up a mib-view without mask.

Command Syntax
set protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **mask** <*mask*>

delete protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **mask**

Parameter

Parameter	Description
mib-view <*view-name*>	Specifies the view name. The value is a string.
subtree <*oidtree*>	Specifies the OID for the MIB subtree. oid-tree can be the OID (such as 1.4.5.3.1) . **NOTE:** It must be a valid MIB subtree.
mask <*mask*>	Subtree mask in hexadecimal format with an even character.

Example

•This example configures a mib-view view1 with mask ff.

```
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1 mask ff
admin@XorPlus# commit
```

set protocols snmp v3 mib-view subtree type

The **set protocols snmp v3 mib-view subtree type** command configures type of a MIB view.

Command Syntax
set protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **type** <**excluded | included**>

delete protocols snmp v3 mib-view <*view-name*> **subtree** <*oidtree*> **type**

Parameter

•<text1> the name of the mib-view

•<text2> a dotted numeric oid

•<type> include or exclude a subtree

- **excluded** exclude the subtree
- **included** include the subtree

Parameter	Description
mib-view <*view-name*>	Specifies the view name. The value is a string.
subtree <*oidtree*>	Specifies the OID for the MIB subtree. oid-tree can be the OID (such as 1.4.5.3.1) . **NOTE:** It must be a valid MIB subtree.
type <**excluded | included**>	Specifies the MIB view type: • **excluded**: Excludes the MIB subtree. • **included**: Includes the MIB subtree.

Usage Guidelines

You can specify the MIB view based on the following rules:

- **excluded**: If a few MIB objects on the device or some objects in the current MIB view do not or no longer need to be managed by the NM station, **excluded** needs to be specified in the command to exclude these MIB objects.
- **included**: If a few MIB objects on the device or some objects in the current MIB view need to be managed by the NM station, **included** needs to be specified in the command to include these MIB objects.

Example

•This example includes 1.3.6.1.2.1 in the view1.

```
admin@XorPlus# set protocols snmp v3 mib-view view1 subtree 1.3.6.1.2.1 type included
admin@XorPlus# commit
```

set protocols snmp trap-group source-interface

The **set protocols snmp trap-group source-interface** command configures the source interface from which traps are sent.

Command Syntax

set protocols snmp trap-group source-interface <*source-interface*>

Parameter

Parameter	Description
source-interface <*source-interface*>	Specifies the source interface. The value could be **eth0**, loopback interface, routed interface, sub-interface or VLAN interface.

Usage Guidelines

You can run this command to specify the source interface on the device from which traps are sent. The specified source interface is used to derive the source IP address for the SNMP traps sent, so that traps received from each switch will always have a single consistent source IP address. To ensure device security, it is recommended that you set the source interface to the loopback interface.

Example

- Configure the loopback interface as the source interface from which traps are sent.

```
admin@Xorplus# set l3-interface loopback lo address 10.226.14.201 prefix-length 32
admin@Xorplus# set protocols snmp trap-group source-interface lo
admin@Xorplus# commit
```

set protocols snmp community

The **set protocols snmp community** command creates an SNMPv1 or SNMPv2c community name.

Command Syntax
set protocols snmp community <*community-name*>
delete protocols snmp community <*community-name*>

Parameter

Parameter	Description
community <*community-name*>	Specifies the name of a community. The value is a string.

Example

•This example configures a community name.

```
admin@XorPlus# set protocols snmp community comm1
admin@XorPlus# commit
```

set protocols snmp community authorization

The **set protocols snmp community authorization** command configures the authorization for an SNMP community.

Command Syntax
set protocols snmp community <*community-name*> **authorization** <**read-only | read-write**>
delete protocols snmp community <*community-name*> **authorization**

Parameter

Parameter	Description
community <*community-name*>	Specifies the name of a community. The value is a string.
authorization <**read-only	read-write**>	Specifies the authorization for an SNMP community. • **read-only**: Indicates that the community with a specified name has the read-only rights. • **read-write**: Indicates that the community with a specified name has the read-write rights.

Example

•This example configures the authorization for an SNMP community.

```
admin@XorPlus# set protocols snmp community comm1 authorization read-only
admin@XorPlus# commit
```

set protocols snmp community clients

The **set protocols snmp community clients** command configures the an SNMP client.

Command Syntax
set protocols snmp community <*community-name*> **clients** <*IP_address*>
delete protocols snmp community <*community-name*> **clients** <*IP_address*>

Parameter

Parameter	Description
community <*community-name*>	Specifies the name of a community. The value is a string.
clients <*IP_address*>	Specifies the IPv4 address of the SNMP client.

Example

•This example configures the an SNMP client.

```
admin@XorPlus# set protocols snmp community comm1 clients 10.10.10.1
admin@XorPlus# commit
```

set protocols snmp contact

The **set protocols snmp contact** command configures the contact information for system maintenance. If a device fails, maintenance engineer can contact the vendor for device maintenance.

Command Syntax
set protocols snmp contact <*contact*>
delete protocols snmp contact

Parameter

Parameter	Description
contact <*contact*>	Specifies contact information of system maintenance. The value is a string.

Example

•This example configures the contact information for system maintenance.

```
admin@XorPlus# set protocols snmp contact support.pica8.com
admin@XorPlus# commit
```

set protocols snmp location

The **set protocols snmp location** command configures the physical location information of the device.

Command Syntax
set protocols snmp location <*location*>
delete protocols snmp location

Parameter

Parameter	Description
location <*location*>	Specifies the physical location information of the device. The value is a string.

Example

•This example configures the physical location information of the device.

```
admin@XorPlus# set protocols snmp location CA:USA
admin@XorPlus# commit
```

Mirror Configuration Commands

- set interface ethernet-switching-options analyzer input
- set interface ethernet-switching-options analyzer output
- set interface ethernet-switching-options analyzer erspan input
- set interface ethernet-switching-options analyzer erspan output source-ip
- set interface ethernet-switching-options analyzer erspan output dest-ip
- set interface ethernet-switching-options analyzer erspan output vrf
- run show analyzer
- set firewall filter sequence then erspan source-ip
- set firewall filter sequence then erspan dest-ip
- set firewall filter sequence then erspan vrf
- set firewall filter sequence then erspan ttl

set interface ethernet-switching-options analyzer input

Port mirroring, is the duplication of traffic from a set of source ports onto a destination port. User can configure port mirroring to monitor and analyze source port traffic.

The **set interface ethernet-switching-options analyzer input** command configures source port, traffics of which need to be monitored. User can use the **set interface ethernet-switching-options analyzer output** command configure destination port.

Command Syntax

set interface ethernet-switching-options analyzer <*string*> **input** <**ingress | egress**> <*port*>

delete interface ethernet-switching-options analyzer <*string*> **input** <**ingress | egress**> <*port*>

Parameter

Parameter	Description
<*string*>	Specifies the name of a mirror, should consist of letters and/or numerals.
<**ingress	egress**>	Specifies the traffic direction of a source port.
<*port*>	Specifies ethernet switching port identifier of the source port.

NOTE :

- For Tomahawk platform switches, port mirroring can not be applied on both direction of the same source interface, that is, you can configure either ingress or egress traffic on the same source interface.
- One chassis switch supports a maximum of four input rules. For example, the following configurations are two input rules of analyzer 111 for the same source interface ge-1/1/3 of two different directions, ingress and egress.

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3

Example

• Configure ge-1/1/3 as the mirrored port, and ge-1/1/4 as the observing port.

```
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 output ge-1/1/4
admin@XorPlus# commit
```

set interface ethernet-switching-options analyzer output

Port mirroring, is the duplication of traffic from a set of source ports onto a destination port. User can configure port mirroring to monitor and analyze source port traffic.

The **set interface ethernet-switching-options analyzer output** command configures destination port, as the observing port of port mirroring. User can use the **set interface ethernet-switching-options analyzer input** command configure source port.

Command Syntax
set interface ethernet-switching-options analyzer <*string*> **output** <*port*>
delete interface ethernet-switching-options analyzer <*string*> **output** <*port*>

Parameter

Parameter	Description
<*string*>	Specifies the name of a mirror, should consist of letters and/or numerals.
<*port*>	Specifies ethernet switching port identifier of the destination port.

NOTE :

- For Tomahawk platform switches, port mirroring can not be applied on both direction of the same source interface, that is, you can configure either ingress or egress traffic on the same source interface.
- One chassis switch supports a maximum of four input rules. For example, the following configurations are two input rules of analyzer 111 for the same source interface ge-1/1/3 of two different directions, ingress and egress.

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3

  admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3

Example
• Configure ge-1/1/3 as the mirrored port, and ge-1/1/4 as the observing port.

```
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input ingress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 input egress ge-1/1/3
admin@XorPlus# set interface ethernet-switching-options analyzer 111 output ge-1/1/4
admin@XorPlus# commit
```

set interface ethernet-switching-options analyzer erspan input

The **set interface ethernet-switching-options analyzer erspan input** command configures the input port of ERSPAN. Parameter *ingress* indicates mirroring traffic in the inbound direction of the input port, *egress* indicates mirroring traffic in the outbound direction of the input port. You can configure to mirror both the ingress and egress traffic at the same time or only one direction.

The **delete interface ethernet-switching-options analyzer erspan input** command deletes the configuration.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan input ingress**<*port-name*>

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan input egress**<*port-name*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
<*port-name*>	Specifies the input port on which the traffic will be mirrored. Only physical interfaces are supported, any other interfaces, such as LAG interface, VLAN interfaces, are not supported.

Example

- The following example commands mirror all packets that te-1/1/4 receives, and copy and transmit the packets from source IP address 100.1.1.1 to destination IP address 200.1.1.2 through a GRE tunnel:

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan input ingress te-1/1/4
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output source-ip 100.1.1.1
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output dest-ip 200.1.1.2
admin@Xorplus# commit
```

set interface ethernet-switching-options analyzer erspan output source-ip

The **set interface ethernet-switching-options analyzer erspan output source-ip** command configures the source IPv4 address for ERSPAN encapsulation.

The **delete interface ethernet-switching-options analyzer erspan output source-ip** command deletes the configuration.

> **NOTE:**
> The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output source-ip** <*source-ipv4*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
source-ip <*source-ipv4*>	Specifies the source IPv4 address for the IP header encapsulation in the outer layer of the GRE message.

Example

- The following example commands mirror all packets that te-1/1/4 receives, and copy and transmit the packets from source IP address 100.1.1.1 to destination IP address 200.1.1.2 through a GRE tunnel:

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan input ingress te-1/1/4
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output source-ip 100.1.1.1
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output dest-ip 200.1.1.2
admin@Xorplus# commit
```

set interface ethernet-switching-options analyzer erspan output dest-ip

The **set interface ethernet-switching-options analyzer erspan output dest-ip** command configures the destination IP address for ERSPAN encapsulation.

The **delete interface ethernet-switching-options analyzer erspan output dest-ip** command deletes the configuration.

NOTEs:

- The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.
- The specified destination IP address should be configured the same as the IP address of the remote Data Monitoring Server to ensure the destination is reachable for the mirrored messages.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output dest-ip** <*dest-ipv4*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
dest-ip <*dest-ipv4*>	Specifies the destination IPv4 address for the IP header encapsulation in the outer layer of the GRE message.

Example

- The following example commands mirror all packets that te-1/1/4 receives, and copy and transmit the packets from source IP address 100.1.1.1 to destination IP address 200.1.1.2 through a GRE tunnel:

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan input ingress te-1/1/4
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output source-ip 100.1.1.1
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output dest-ip 200.1.1.2
admin@Xorplus# commit
```

set interface ethernet-switching-options analyzer erspan output vrf

The **set interface ethernet-switching-options analyzer erspan output vrf** command configures the VRF of the ERSPAN GRE tunnel of destination interface. Note that you have to ensure the remote data monitoring server is route reachable in the VRF.

The **delete interface ethernet-switching-options analyzer erspan output vrf** command deletes the configuration.

Command Syntax

set interface ethernet-switching-options analyzer <*mirror-name*> **erspan output vrf** <*vrf-name*>

Parameters

Parameter	Description
analyzer <*mirror-name*>	Specifies a name of the ERSPN. The value is a string.
vrf <*vrf-name*>	Specifies the VRF name of the GRE tunnel for ERSPAN.

Example

- Configure VRF of the GRE tunnel for ERSPAN.

```
admin@Xorplus# set interface ethernet-switching-options analyzer 111 erspan output vrf vrf1
admin@Xorplus# commit
```

run show analyzer

The **run show analyzer** command is used to view the mirroring information.

Command Syntax

run show analyzer [<*mirror-name*>]

Parameter

Parameter	Description
<*mirror-name*>	Optional. Specifies a name of the ERSPN. The value is a string.

Example

- View mirror configuration information.

```
admin@PICOS# run show analyzer
Analyzer name: 111
Erspan Output:
       state: UP
       source-ip: 10.10.10.1
       dest-ip: 20.20.20.1
       output-port: ge-1/1/3
       tagged vlan:
       vrf:
Ingress monitored interfaces: <ge-1/1/1>
Egress monitored interfaces:

Analyzer name: 3
Output interface: <ge-1/1/5>
Ingress monitored interfaces: <ge-1/1/1>
Egress monitored interfaces:

admin@SwitchB# run show analyzer 111
Analyzer name: 111
Output interface: <ge-1/1/2>
Ingress monitored interfaces: <ge-1/1/1>
Egress monitored interfaces: <ge-1/1/1>
```

set firewall filter sequence then erspan source-ip

The **set firewall filter sequence then erspan source-ip** command configures the source IP address for ACL-based ERSPAN encapsulation for the packets matching the ACL rule.

If ACL-based ERSPAN is configured, PICOS copies service flows matching the rules to the output port, and then forwards the mirrored messages to the remote monitoring device through the GRE tunnel for analysis and monitoring. This command configures the source IP address of the GRE tunnel.

The **delete firewall filter sequence then erspan source-ip** command deletes the configuration.

> **NOTE:**
> The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan source-ip** <*source-ip*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
source-ip <*source-ip*>	Specifies the source IP address of the GRE tunnel of ERSPAN destination interface.

Example

- The following example commands mirror the packets matching the ACL rule that te-1/1/1 receives, and copy and transmit the packets from source IP address 4.4.4.4 to destination IP address 8.8.8.8through a GRE tunnel:

```
admin@Xorplus# set firewall filter f1 sequence 1 from protocol tcp
admin@Xorplus# set firewall filter f1 sequence 1 from source-address-ipv4 1.1.1.1/32
admin@Xorplus# set firewall filter f1 input interface te-1/1/1
admin@Xorplus# set firewall filter f1 sequence 1 then erspan source-ip 4.4.4.4
admin@Xorplus# set firewall filter f1 sequence 1 then erspan dest-ip 8.8.8.8
admin@Xorplus# commit
```

set firewall filter sequence then erspan dest-ip

The **set firewall filter sequence then erspan dest-ip** command configures the destination IP address for ACL-based ERSPAN encapsulation for the packets matching the ACL rule.

If ACL-based ERSPAN is configured, PICOS copies service flows matching the rules to the output port, and then forwards the mirrored messages to the remote monitoring device through the GRE tunnel for analysis and monitoring. This command configures the destination IP address of the GRE tunnel.

The **delete interface ethernet-switching-options analyzer erspan output dest-ip** command deletes the configuration.

NOTEs:

- The configured source IPv4 address and destination IPv4 address are used for the IP header encapsulation in the outer layer of the GRE message. Users have to configure the routing protocol to ensure the devices at both ends of the GRE tunnel are route reachable.
- The specified destination IP address should be configured the same as the IP address of the remote Data Monitoring Server to ensure the destination is reachable for the mirrored messages.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan dest-ip** <*dest-ip*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
dest-ip <*dest-ip*>	Specifies the destination IP address of the GRE tunnel of ERSPAN destination interface.

Example

- The following example commands mirror the packets matching the ACL rule that te-1/1/1 receives, and copy and transmit the packets from source IP address 4.4.4.4 to destination IP address 8.8.8.8 through a GRE tunnel:

```
admin@Xorplus# set firewall filter f1 sequence 1 from protocol tcp
admin@Xorplus# set firewall filter f1 sequence 1 from source-address-ipv4 1.1.1.1/32
admin@Xorplus# set firewall filter f1 input interface te-1/1/1
admin@Xorplus# set firewall filter f1 sequence 1 then erspan source-ip 4.4.4.4
admin@Xorplus# set firewall filter f1 sequence 1 then erspan dest-ip 8.8.8.8
admin@Xorplus# commit
```

set firewall filter sequence then erspan vrf

The **set firewall filter sequence then erspan vrf** command configures the VRF of the ACL-based ERSPAN GRE tunnel. Note that you have to ensure the remote data monitoring server is route reachable in the VRF.

The **delete firewall filter sequence then erspan vrf** command deletes the configuration.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan vrf** <*vrf-name*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
vrf <*vrf-name*>	Specifies the VRF of the ACL-based ERSPAN GRE tunnel. The value is a string.

Example

- Configure VRF of the GRE tunnel for ACL-based ERSPAN.

```
admin@Xorplus# set firewall filter f1 sequence 1 then erspan vrf vrf1
admin@Xorplus# commit
```

set firewall filter sequence then erspan ttl

The **set firewall filter sequence then erspan ttl** command configures the Time-To-Life (TTL) value of the ACL-based ERSPAN packets.

The **delete firewall filter sequence then erspan ttl** command deletes the configuration.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then erspan ttl** <*ttl-value*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies the filter name. The value is a string.
sequence <*number*>	Specifies the filter sequence number. The value is an integer that ranges from 0 to 9999.
ttl <*ttl-value*>	Specifies the TTL value of the ACL-based ERSPAN packets. The value is an integer that ranges from 1 to 255. The default value is 255.

Example

- Configure TTL value of the ACL-based ERSPAN packets to 64.

```
admin@Xorplus# set firewall filter f1 sequence 1 then erspan ttl 64
admin@Xorplus# commit
```

RMON Commands

- run show rmon alarms
- run show rmon eventlog
- run show rmon events
- run show rmon history
- run show rmon statistics
- set protocols snmp rmon alarm falling-event-index
- set protocols snmp rmon alarm falling-threshold
- set protocols snmp rmon alarm interval
- set protocols snmp rmon alarm owner
- set protocols snmp rmon alarm rising-event-index
- set protocols snmp rmon alarm rising-threshold
- set protocols snmp rmon alarm sample-type
- set protocols snmp rmon alarm variable
- set protocols snmp rmon event community
- set protocols snmp rmon event description
- set protocols snmp rmon event owner
- set protocols snmp rmon event type
- set protocols snmp rmon history buckets
- set protocols snmp rmon history interface
- set protocols snmp rmon history interval
- set protocols snmp rmon history owner
- set protocols snmp rmon statistics interface
- set protocols snmp rmon statistics owner

run show rmon alarms

The **run show rmon alarms** command is used to view RMON alarms information.

Command Syntax

run show rmon alarms [<*entry-index*>]

Parameter

Parameter	Description
[<*entry-index*>]	Optional. Specifies the RMON alarms table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON alarms information.

```
admin@PICOS# run show rmon alarms
Entry 1 is active, and owned by monitor
    Monitors 1.3.6.1.2.1.16.1.1.1.4.1 every 10 seconds
    Taking absolute samples, last value was 369804
    Rising threshold is 1000000000, assigned to event 1
    Falling threshold is 1000000000, assigned to event 1
    On startup enable rising or falling alarm
```

run show rmon eventlog

The **run show rmon eventlog** command is used to view RMON event log information.

Command Syntax

run show rmon eventlog [*<entry-index>*]

Parameter

Parameter	Description
[*<entry-index>*]	Optional. Specifies the RMON event log table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON event log information.

```
admin@PICOS# run show rmon eventlog
Entry 1 owned by monitor is VALID.
    Generates eventLog 1.1 at 0:01:19.
    Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarmEntry 1, equal or lesser than 1000000000 with alarm v
```

run show rmon events

The **run show rmon events** command is used to view RMON event information.

Command Syntax

run show rmon events [*<entry-index>*]

Parameter

Parameter	Description
[*<entry-index>*]	Optional. Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON event information.

```
admin@PICOS# run show rmon events
Entry 1 is active, and owned by monitor,
    Description is test,
    Event firing causes trap to community public,
    Last event fired at 0:01:19,
    Current uptime 1:02:17.
```

run show rmon history

The **run show rmon history** command is used to view RMON history statistics information.

Command Syntax

run show rmon history [*<entry-index>*]

Parameter

Parameter	Description
[*<entry-index>*]	Optional. Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.

Example

- View RMON history statistics information.

```
admin@PICOS# run show rmon history
Entry 3 on ge-1/1/21 is active, and owned by monitor,
    Monitors ifIndex.21 every 10 seconds, bucket is 50,
        Sample # 1 began measuring at 0:43:22
            Received 576000 octets, 9000 packets,
            0 broadcast and 9000 multicast packets,
            0 undersized and 0 oversized packets,
            0 fragments and 0 jabbers,
            0 CRC alignment errors and 0 collisions.
            network utilization is estimated at 0
```

run show rmon statistics

The **run show rmon statistics** command is used to view RMON Ethernet statistics information.

Command Syntax

run show rmon statistics [<*entry-index*>]

Parameter

Parameter	Description
[<*entry-index*>]	Optional. Specifies the RMON statistics table index. The value is an integer that ranges from 1 to 255.

Example

- View RMON Ethernet statistics information.

```
admin@PICOS# run show rmon statistics
Entry 1 on ge-1/1/4 is active, and owned by monitor,
    Monitors ifIndex.4 which has
    Received 354601 octets, 3643 packets,
    0 broadcast and 0 multicast packets,
    0 undersized and 0 oversized packets,
    0 fragments and 0 jabbers,
    0 CRC alignment errors and 0 collisions.
    dropped packet events (due to lack of resources):0.
    packets received of length (in octets):
        64: 0, 65-127: 3524, 128-255: 119,
        256-511: 0, 512-1023: 0, 1024-1518: 0
```

set protocols snmp rmon alarm falling-event-index

The **set protocols snmp rmon alarm falling-event-index** command configures the event to fire when the alarm falling threshold is crossed.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **falling-event-index** <*alarmFallingEventIndex*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
falling-event-index <*alarmFallingEventIndex*>	Specifies the event to fire when the alarm falling threshold is crossed. The value is an integer that is configured in command **set protocols snmp rmon event** <*entry-index*> *XX*. When configured to 0, it indicates no event has been specified, so no action will be taken when the alarm threshold is exceeded.

Example

- Configure the event to fire when the falling threshold is crossed.

```
admin@PICOS# set protocols snmp rmon alarm 1 falling-event-index 5
admin@PICOS# commit
```

set protocols snmp rmon alarm falling-threshold

The **set protocols snmp rmon alarm falling-threshold** command configures the falling threshold of the RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **falling-threshold** <*alarmFallingThreshold*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
falling-threshold <*alarmFallingThreshold*>	Specifies the falling threshold. The value is an integer that ranges from 0 to 2147483647.

Usage Guidelines

Rising threshold and falling threshold are a pair of values for a monitoring object, both values need to be configured for the same alarm entry.

In the following configuration example, the alarm event is triggered when the rising threshold 600 is exceeded, and the alarm event is triggered again when the monitoring value falls back to the falling threshold 400.

```
admin@Switch# set protocols snmp rmon alarm 1 rising-threshold 600
admin@Switch# set protocols snmp rmon alarm 1 rising-event-index 1
admin@Switch# set protocols snmp rmon alarm 1 falling-threshold 400
admin@Switch# set protocols snmp rmon alarm 1 falling-event-index 1
```

Example

- Configure the falling threshold of the RMON alarm to 600.

```
admin@PICOS# set protocols snmp rmon alarm 1 falling-threshold 600
admin@PICOS# commit
```

set protocols snmp rmon alarm interval

The **set protocols snmp rmon alarm interval** command configures the sampling interval of RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **interval** <*interval*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
interval <*interval*>	Specifies the sampling interval for RMON alarm. The value is an integer, in seconds, that ranges from 10 to 3600.

Example

- Configure the sampling interval of RMON alarm to 20 seconds.

```
admin@PICOS# set protocols snmp rmon alarm 1 interval 20
admin@PICOS# commit
```

set protocols snmp rmon alarm owner

The **set protocols snmp rmon alarm owner** command configures the owner's name of the RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **owner** <*owner*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
owner <*owner*>	Specifies the owner's name of the RMON alarm. The value is a string.

Example

- Configure the owner for the RMON alarm.

```
admin@PICOS# set protocols snmp rmon alarm 1 owner public
admin@PICOS# commit
```

set protocols snmp rmon alarm rising-event-index

The **set protocols snmp rmon alarm rising-event-index** command configures the event to fire when the alarm rising threshold is crossed.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **rising-event-index** <*alarmRisingEventIndex*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 0 to 65535.
rising-event-index <*alarmRisingEventIndex*>	Specifies the event to fire when the alarm rising threshold is crossed. The value is an integer that is configured in command **set protocols snmp rmon event** <*entry-index*> *XX*. When configured to 0, it indicates no event has been specified, so no action will be taken when the alarm threshold is exceeded.

Example

- Configure the event to fire when the rising threshold is crossed.

```
admin@PICOS# set protocols snmp rmon alarm 1 rising-event-index 5
admin@PICOS# commit
```

set protocols snmp rmon alarm rising-threshold

The **set protocols snmp rmon alarm rising-threshold** command configures the rising threshold of the RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **rising-threshold** <*alarmRisingThreshold*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
rising-threshold <*alarmRisingThreshold*>	Specifies the rising threshold. The value is an integer that ranges from 0 to 2147483647.

Usage Guidelines

Rising threshold and falling threshold are a pair of values for a monitoring object, both values need to be configured for the same alarm entry.

In the following configuration example, the alarm event is triggered when the rising threshold 600 is exceeded, and the alarm event is triggered again when the monitoring value falls back to the falling threshold 400.

```
admin@Switch# set protocols snmp rmon alarm 1 rising-threshold 600
admin@Switch# set protocols snmp rmon alarm 1 rising-event-index 1
admin@Switch# set protocols snmp rmon alarm 1 falling-threshold 400
admin@Switch# set protocols snmp rmon alarm 1 falling-event-index 1
```

Example

- Configure the rising threshold of the RMON alarm to 600.

```
admin@PICOS# set protocols snmp rmon alarm 1 rising-threshold 600
admin@PICOS# commit
```

set protocols snmp rmon alarm sample-type

The **set protocols snmp rmon alarm sample-type** command configures the sampling type of RMON alarm.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **sample-type** <**absolute** | **delta**>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
sample-type <**absolute** | **delta**>	Specifies the sampling type for RMON alarm. The value could be **absolute** or **delta**. • **absolute**: If the sample type is absolute, this value will be the sampled value at the end of the period. • **delta**: If the sample type is delta, this value will be the difference between the samples at the beginning and end of the period.

Example

- Configure the sampling type of RMON alarm to **delta**.

```
admin@PICOS# set protocols snmp rmon alarm 1 sample-type delta
admin@PICOS# commit
```

set protocols snmp rmon alarm variable

The **set protocols snmp rmon alarm variable** command configures SNMP MIB OID of the RMON alarm monitoring object.

The **delete protocols snmp rmon alarm** command deletes the configuration. Users need to delete the RMON alarm entry to remove this configuration.

Command Syntax

set protocols snmp rmon alarm <*entry-index*> **variable** <*oid-variable*>

delete protocols snmp rmon alarm <*entry-index*>

Parameters

Parameter	Description
alarm <*entry-index*>	Specifies the RMON alarm table index. The value is an integer that ranges from 1 to 65535.
variable <*oid-variable*>	Specifies SNMP MIB OID of the RMON alarm. The value is a string.

Example

- Configure a RMON alarm for OID of 1.3.6.1.2.1.16.1.1.1.4.1.

```
admin@PICOS# set protocols snmp rmon alarm 1 variable 1.3.6.1.2.1.16.1.1.1.4.1
admin@PICOS# commit
```

set protocols snmp rmon event community

The **set protocols snmp rmon event community** command configures the community for the RMON event.

Note:

The **community** setting here should be consistent with the value of **community** and **security-name** in SNMP trap configuration.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **community** <*community*>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
community <*community*>	Specifies the name of a community. The value is a string. The default value is **public**.

Example

- Configure the community for the RMON event.

```
admin@PICOS# set protocols snmp rmon event 1 community comm1
admin@PICOS# commit
```

set protocols snmp rmon event description

The **set protocols snmp rmon event description** command configures the description for the RMON event.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **description** <*event_description*>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
description <*event_description*>	Specifies the description for the RMON event. The value is a string.

Example

- Configure the description for the RMON event.

```
admin@PICOS# set protocols snmp rmon event 1 description AlarmEvent
admin@PICOS# commit
```

set protocols snmp rmon event owner

The **set protocols snmp rmon event owner** command configures the owner's name of the RMON event.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **owner** <*owner*>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
owner <*owner*>	Specifies the owner's name of the RMON event. The value is a string.

Example

- Configure the owner for the RMON event.

```
admin@PICOS# set protocols snmp rmon event 1 owner public
admin@PICOS# commit
```

set protocols snmp rmon event type

The **set protocols snmp rmon event type** command configures the RMON event action type.

The **delete protocols snmp rmon event** command deletes the configuration. Users need to delete the RMON event entry to remove this configuration.

Command Syntax

set protocols snmp rmon event <*entry-index*> **type** <**none** | **log** | **trap** | **log-trap**>

delete protocols snmp rmon event <*entry-index*>

Parameters

Parameter	Description
event <*entry-index*>	Specifies the RMON event table index. The value is an integer that ranges from 1 to 65535.
type <**none** | **log** | **trap** | **log-trap**>	Specifies RMON event action type. The value could be **none**, **log**, **trap** or **log-trap**. • **none**: Nothing will be done if the event is triggered. • **log**: If the event is triggered, an entry will be made in the logTable. • **trap**: If the event is triggered, an SNMP trap will be sent to the management station. • **log-trap**: If the event is triggered, both the log and trap action will be taken.

Usage Guidelines

When type is **trap** or **log-trap**, you need to configure SNMP trap function.

Example

- Configure the RMON event action type to **log**.

```
admin@PICOS# set protocols snmp rmon event 1 type log
admin@PICOS# commit
```

set protocols snmp rmon history buckets

The **set protocols snmp rmon history buckets** command configures the history statistics table capacity, that is, the maximum number of records that the history table can hold.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **buckets** <*number*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
buckets <*number*>	Specifies the history statistics table capacity, that is, the maximum number of records that the history table can hold. The value is an integer that ranges from 1 to 65535.

Example

- Configure the history statistics table capacity to 100.

```
admin@PICOS# set protocols snmp rmon history 1 buckets 100
admin@PICOS# commit
```

set protocols snmp rmon history interface

The **set protocols snmp rmon history interface** command configures RMON history statistics on a specified interface.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **interface** <*interface-name*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
interface <*interface-name*>	Specifies the interface for RMON history statistics. The value could be a physical interface or LAG interface.

Usage Guidelines

RMON historical statistics collects statistics periodically, but only the latest statistics are stored. The maximum number of records that the history table can hold is configured by command **set protocols snmp rmon history** <*entry-index*> **buckets** <*number*>.

Example

- Configure RMON history statistics on interface ge-1/1/1.

```
admin@PICOS# set protocols snmp rmon history 1 interface ge-1/1/1
admin@PICOS# commit
```

set protocols snmp rmon history interval

The **set protocols snmp rmon history interval** command configures the sampling interval of RMON history statistics.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **interval** <*interval*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
interval <*interval*>	Specifies the sampling interval for RMON history statistics. The value is an integer, in seconds, that ranges from 10 to 3600.

Example

- Configure the sampling interval of RMON history statistics to 20 seconds.

```
admin@PICOS# set protocols snmp rmon history 1 interval 20
admin@PICOS# commit
```

set protocols snmp rmon history owner

The **set protocols snmp rmon history owner** command configures the owner's name of the RMON history statistics table.

The **delete protocols snmp rmon history** command deletes the configuration. Users need to delete the RMON history statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon history <*entry-index*> **owner** <*string*>

delete protocols snmp rmon history <*entry-index*>

Parameters

Parameter	Description
history <*entry-index*>	Specifies the RMON history statistics table index. The value is an integer that ranges from 1 to 65535.
owner <*string*>	Specifies the owner's name of the RMON statistics table. The value is a string.

Example

- Configure the owner's name of the RMON history statistics table.

```
admin@PICOS# set protocols snmp rmon history 1 owner owner_pica8
admin@PICOS# commit
```

set protocols snmp rmon statistics interface

The **set protocols snmp rmon statistics interface** command configures RMON ethernet statistics on a specified interface. After the statistics table entry is configured under the specified interface, the system continuously gathers statistics for the number of messages on the interface.

The **delete protocols snmp rmon statistics** command deletes the configuration. Users need to delete the RMON ethernet statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon statistics <*entry-index*> **interface** <*interface-name*>

delete protocols snmp rmon statistics <*entry-index*>

Parameters

Parameter	Description
statistics <*entry-index*>	Specifies the RMON ethernet statistics table index. The value is an integer that ranges from 1 to 255.
interface <*interface-name*>	Specifies the interface for RMON ethernet statistics. The value could be a physical interface or LAG interface.

Example

- Configure RMON ethernet statistics on interface ge-1/1/1.

```
admin@PICOS# set protocols snmp rmon statistics 1 interface ge-1/1/1
admin@PICOS# commit
```

set protocols snmp rmon statistics owner

The **set protocols snmp rmon statistics owner** command configures the owner's name of the RMON ethernet statistics table.

The **delete protocols snmp rmon statistics** command deletes the configuration. Users need to delete the RMON ethernet statistics entry to remove this configuration.

Command Syntax

set protocols snmp rmon statistics <*entry-index*> **owner** <*string*>

delete protocols snmp rmon statistics <*entry-index*>

Parameters

Parameter	Description
statistics <*entry-index*>	Specifies the RMON ethernet statistics table index. The value is an integer that ranges from 1 to 255.
owner <*string*>	Specifies the owner's name of the RMON ethernet statistics table. The value is a string.

Example

- Configure the owner's name of the RMON ethernet statistics table.

```
admin@PICOS# set protocols snmp rmon statistics 1 owner owner_pica8
admin@PICOS# commit
```

RESTCONF Commands

- set protocols restconf
- set protocols restconf port
- set protocols restconf traceoptions flag config disable
- set protocols restconf traceoptions flag all disable
- set protocols restconf traceoptions flag datastore disable

set protocols restconf

The **set protocols restconf** command enables RESTCONF function on RESTCONF server. By default, RESTCONF is disabled.

The **delete protocols restconf** command disables RESTCONF on RESTCONF server.

Command Syntax

set protocols restconf

delete protocols restconf

Parameters

None.

Example

- Enable RESTCONF on RESTCONF server.

```
admin@PICOS# set protocols restconf
admin@PICOS# commit
```

set protocols restconf port

The **set protocols restconf port** command configures RESTCONF service listening port on RESTCONF server. By default, the RESTCONF service port number is 443.

The **delete protocols restconf port** command restores the configuration to the default value on RESTCONF server.

> **NOTE**:
>
> The RESTCONF service listening port in the HTTP request URL sent by RESTCONF Client needs to be consistent with the port configured on the server side.

Command Syntax

set protocols restconf port *<port-number>*

delete protocols restconf port

Parameter

Parameter	Description
port *<port-number>*	Specifies RESTCONF service listening port. The value is an integer that ranges from 1024 to 65535. The default value is 443.

Example

- Configure RESTCONF service listening port to 1024 on RESTCONF server.

```
admin@PICOS# set protocols restconf port 1024
admin@PICOS# commit
```

set protocols restconf traceoptions flag config disable

The **set protocols restconf traceoptions flag config disable** command can be used to enable or disable RESTCONF debugging for configuration tracing.

The **delete protocols restconf traceoptions flag config disable** command deletes the configuration.

Command Syntax

set protocols restconf traceoptions flag config disable <**true | false**>

delete protocols restconf traceoptions flag config disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable RESTCONF debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable RESTCONF debugging for configuration tracing. • **false**: Enable RESTCONF debugging for configuration tracing. By default, RESTCONF debugging for configuration tracing is disabled.

Example

- Enable RESTCONF debugging for configuration tracing.

```
admin@PICOS# set protocols restconf traceoptions flag config disable false
admin@PICOS# commit
```

set protocols restconf traceoptions flag all disable

The **set protocols restconf traceoptions flag all disable** command can be used to enable or disable RESTCONF debugging for tracing all RESTCONF operations.

The **delete protocols restconf traceoptions flag all disable** command deletes the configuration.

Command Syntax

set protocols restconf traceoptions flag all disable <**true | false**>

delete protocols restconf traceoptions flagall disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable RESTCONF debugging for tracing all RESTCONF operations. The value could be **true** or **false**. • **true**: Disable RESTCONF debugging for tracing all RESTCONF operations. • **false**: Enable RESTCONF debugging for tracing all RESTCONF operations. By default, RESTCONF debugging for tracing all RESTCONF operations is disabled.

Example

- Enable RESTCONF debugging for tracing all RESTCONF operations.

```
admin@PICOS# set protocols restconf traceoptions flag all disable false
admin@PICOS# commit
```

set protocols restconf traceoptions flag datastore disable

The **set protocols restconf traceoptions flag datastore disable** command can be used to enable or disable debugging about the RESTCONF datastore operation.

The **delete protocols restconf traceoptions flag datastore disable** command deletes the configuration.

Command Syntax

set protocols restconf traceoptions flag datastore disable <**true | false**>

delete protocols restconf traceoptions flag datastore disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable debugging about the RESTCONF datastore operation. The value could be **true** or **false**. • **true**: Disable debugging about the RESTCONF datastore operation. • **false**: Enable debugging about the RESTCONF datastore operation. By default, debugging about the RESTCONF datastore operation is disabled.

Example

- Enable debugging about the RESTCONF datastore operation.

```
admin@PICOS# set protocols restconf traceoptions flag datastore disable false
admin@PICOS# commit
```

run show system boot-messages

The **run show system boot-message** command displays information about boot time messages. The command displays copyright, up time, revision, using MPC85 xx CDS machine description, etc.

Command Syntax
run show system boot-messages

Example
• This example demonstrates how to show system boot-messages:

```
admin@XorPlus# run show system boot-messages
Copyright (c) 2009-2014 Pica8 Inc.
All rights reserved.
Up time: 13:03:50
revision: 2.6.27
Using MPC85xx CDS machine description
Memory CAM mapping: CAM0=256Mb, CAM1=256Mb, CAM2=0Mb residual: 0Mb
Linux version 2.6.27 (root@dev-18) (gcc version 4.2.2) #49 Fri Apr 25 11:19:13 CST 2014
Found legacy serial port 0 for /soc8541@e0000000/serial@4500
  mem=e0004500, taddr=e0004500, irq=0, clk=330000000, speed=0
console [udbg0] enabled
Found FSL PCI host bridge at 0x00000000e0008000. Firmware bus number: 0->0
PCI host bridge /pci@e0008000 (primary) ranges:
 MEM 0x0000000080000000..0x000000009fffffff -> 0x0000000080000000
  IO 0x00000000e2000000..0x00000000e20fffff -> 0x0000000000000000
Top of RAM: 0x20000000, Total RAM: 0x20000000
Memory hole size: 0MB
Zone PFN ranges:
  DMA      0x00000000 -> 0x00020000
  Normal   0x00020000 -> 0x00020000
  HighMem  0x00020000 -> 0x00020000
Movable zone start PFN for each node
early_node_map[1] active PFN ranges
    0: 0x00000000 -> 0x00020000
On node 0 totalpages: 131072
free_area_init_node: node 0, pgdat c03cc4d4, node_mem_map c0404000
  DMA zone: 130048 pages, LIFO batch:31
Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 130048
Kernel command line: root=/dev/hda1 rw noinitrd console=ttyS0,115200
mpic: Setting up MPIC " OpenPIC  " version 1.2 at e0040000, max 1 CPUs
mpic: ISU size: 56, shift: 6, mask: 3f
mpic: Initializing for 56 sources
PID hash table entries: 2048 (order: 11, 8192 bytes)
time_init: decrementer frequency = 41.250000 MHz
time_init: processor frequency   = 825.000000 MHz
clocksource: timebase mult[60f83e1] shift[22] registered
clockevent: decrementer mult[a8f] shift[16] cpu[0]
Console: colour dummy device 80x25
Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
High memory: 0k
Memory: 515456k/524288k available (3764k kernel code, 8648k reserved, 132k data, 162k bss, 168k init)
SLUB: Genslabs=12, HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
Calibrating delay loop... 82.43 BogoMIPS (lpj=164864)
 --More--
```

run show system connections

The **run show system connections** command displays information about the system connection activity. It includes servers and established. The command displays Proto, .Recv-q, Send-Q, Local Address, Foreign Address, State, User, and Inode.

Command Syntax
run show system connections

Example
• This example demonstrates how to show system connections:

```
admin@XorPlus# run show system connections
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode
tcp        0      0 127.0.0.1:44992         0.0.0.0:*               LISTEN      11         34882
tcp        0      0 127.0.0.1:41248         0.0.0.0:*               LISTEN      0          1458
tcp        0      0 127.0.0.1:56961         0.0.0.0:*               LISTEN      11         7095
tcp        0      0 127.0.0.1:42946         0.0.0.0:*               LISTEN      0          2614
tcp        0      0 127.0.0.1:43938         0.0.0.0:*               LISTEN      0          1406
tcp        0      0 127.0.0.1:50436         0.0.0.0:*               LISTEN      0          2653
tcp        0      0 127.0.0.1:51622         0.0.0.0:*               LISTEN      0          2620
tcp        0      0 127.0.0.1:54214         0.0.0.0:*               LISTEN      0          2618
tcp        0      0 127.0.0.1:47143         0.0.0.0:*               LISTEN      0          4411
tcp        0      0 127.0.0.1:36455         0.0.0.0:*               LISTEN      0          1462
tcp        0      0 127.0.0.1:39592         0.0.0.0:*               LISTEN      0          1466
tcp        0      0 127.0.0.1:53512         0.0.0.0:*               LISTEN      0          1319
tcp        0      0 127.0.0.1:57354         0.0.0.0:*               LISTEN      0          4257
tcp        0      0 127.0.0.1:33197         0.0.0.0:*               LISTEN      0          4400
tcp        0      0 127.0.0.1:58765         0.0.0.0:*               LISTEN      0          1460
tcp        0      0 127.0.0.1:55985         0.0.0.0:*               LISTEN      0          1456
tcp        0      0 127.0.0.1:56564         0.0.0.0:*               LISTEN      0          2577
tcp        0      0 127.0.0.1:44756         0.0.0.0:*               LISTEN      0          1464
tcp        0      0 127.0.0.1:51957         0.0.0.0:*               LISTEN      0          1468
tcp        0      0 127.0.0.1:44086         0.0.0.0:*               LISTEN      11         66976
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          3364
tcp        0      0 127.0.0.1:51222         0.0.0.0:*               LISTEN      0          2575
tcp        0      0 127.0.0.1:53208         0.0.0.0:*               LISTEN      0          4252
tcp        0      0 127.0.0.1:56441         0.0.0.0:*               LISTEN      0          2616
tcp        0      0 127.0.0.1:37210         0.0.0.0:*               LISTEN      0          4286
tcp        0      0 127.0.0.1:29595         0.0.0.0:*               LISTEN      0          1316
tcp        0      0 127.0.0.1:38492         0.0.0.0:*               LISTEN      0          1454
tcp        0      0 127.0.0.1:52988         0.0.0.0:*               LISTEN      0          1452
tcp        0      0 127.0.0.1:50206         0.0.0.0:*               LISTEN      0          1450
tcp        0      0 127.0.0.1:29595         127.0.0.1:45862         ESTABLISHED 0          2637
tcp        0      0 127.0.0.1:55985         127.0.0.1:34260         ESTABLISHED 0          4295
tcp        0      0 127.0.0.1:57004         127.0.0.1:50206         ESTABLISHED 0          1629
tcp        0      0 127.0.0.1:38841         127.0.0.1:57354         ESTABLISHED 0          4264
tcp        0      0 127.0.0.1:41248         127.0.0.1:33787         ESTABLISHED 0          4271
tcp        0      0 127.0.0.1:29595         127.0.0.1:45845         ESTABLISHED 0          1485
tcp        0      0 127.0.0.1:59503         127.0.0.1:50436         ESTABLISHED 0          2696
tcp        0      0 127.0.0.1:29595         127.0.0.1:45854         ESTABLISHED 0          2579
tcp        0      0 127.0.0.1:54304         127.0.0.1:44086         ESTABLISHED 0          67026
tcp        0      0 127.0.0.1:57039         127.0.0.1:50206         ESTABLISHED 0          4266
tcp        0      0 127.0.0.1:44118         127.0.0.1:43938         ESTABLISHED 0          2222
tcp        0      0 127.0.0.1:43938         127.0.0.1:44162         ESTABLISHED 0          4418
tcp        0      0 127.0.0.1:29595         127.0.0.1:45879         ESTABLISHED 0          4254
tcp        0      0 127.0.0.1:41078         127.0.0.1:37210         ESTABLISHED 0          4292
tcp        0      0 127.0.0.1:41077         127.0.0.1:37210         ESTABLISHED 0          4289
tcp        0      0 127.0.0.1:55264         127.0.0.1:33197         ESTABLISHED 0          27675
tcp        0      0 127.0.0.1:42946         127.0.0.1:59983         ESTABLISHED 0          4441
tcp        0      0 127.0.0.1:50436         127.0.0.1:59503         ESTABLISHED 0          2697
tcp        0      0 127.0.0.1:50436         127.0.0.1:43906         ESTABLISHED 0          7121
```

```
tcp        0      0 127.0.0.1:50206         127.0.0.1:57027         ESTABLISHED 0          2678
tcp        0      0 127.0.0.1:33197         127.0.0.1:55264         ESTABLISHED 0          27676
tcp        0      0 127.0.0.1:29595         127.0.0.1:33590         ESTABLISHED 0          34884
tcp        0      0 127.0.0.1:57887         127.0.0.1:33197         ESTABLISHED 0          4432
tcp        0      0 127.0.0.1:36773         127.0.0.1:56441         ESTABLISHED 0          2641
tcp        0      0 127.0.0.1:57354         127.0.0.1:38841         ESTABLISHED 0          4265
tcp        0      0 127.0.0.1:29595         127.0.0.1:40818         ESTABLISHED 0          67021
tcp        0      0 127.0.0.1:29595         127.0.0.1:45889         ESTABLISHED 0          4288
tcp        0      0 127.0.0.1:45894         127.0.0.1:29595         ESTABLISHED 0          4412
tcp        0      0 127.0.0.1:57883         127.0.0.1:33197         ESTABLISHED 0          4413
tcp        0      0 127.0.0.1:29595         127.0.0.1:45836         ESTABLISHED 0          1323
tcp        0      0 127.0.0.1:35592         127.0.0.1:50436         ESTABLISHED 11         34907
tcp        0      0 127.0.0.1:29595         127.0.0.1:45881         ESTABLISHED 0          4259
tcp        0      0 127.0.0.1:45839         127.0.0.1:29595         ESTABLISHED 0          1469
tcp        0      0 127.0.0.1:59990         127.0.0.1:42946         ESTABLISHED 0          5128
tcp        0      0 127.0.0.1:45854         127.0.0.1:29595         ESTABLISHED 0          2578
tcp        0      0 127.0.0.1:29595         127.0.0.1:45860         ESTABLISHED 0          2632
tcp        0      0 10.10.50.150:22         10.10.50.16:42504       ESTABLISHED 0          6553
tcp        0      0 127.0.0.1:44104         127.0.0.1:43938         ESTABLISHED 0          1409
tcp        0      0 127.0.0.1:42946         127.0.0.1:59988         ESTABLISHED 0          4592
tcp        0      0 127.0.0.1:33590         127.0.0.1:29595         ESTABLISHED 11         34883
tcp        0      0 127.0.0.1:36916         127.0.0.1:51222         ESTABLISHED 0          2680
tcp        0      0 127.0.0.1:45841         127.0.0.1:29595         ESTABLISHED 0          1472
tcp        0      0 127.0.0.1:33197         127.0.0.1:57892         ESTABLISHED 0          4579
tcp        0      0 127.0.0.1:45889         127.0.0.1:29595         ESTABLISHED 0          4287
tcp        0      0 127.0.0.1:57019         127.0.0.1:50206         ESTABLISHED 0          2639
tcp        0      0 127.0.0.1:44239         127.0.0.1:36455         ESTABLISHED 0          2684
tcp        0      0 127.0.0.1:29595         127.0.0.1:45837         ESTABLISHED 0          1408
tcp        0      0 127.0.0.1:45848         127.0.0.1:29595         ESTABLISHED 0          1479
tcp        0      0 127.0.0.1:38492         127.0.0.1:39516         ESTABLISHED 0          2226
tcp        0      0 127.0.0.1:59953         127.0.0.1:42946         ESTABLISHED 0          2675
tcp        0      0 127.0.0.1:60034         127.0.0.1:53512         ESTABLISHED 0          2669
tcp        0      0 127.0.0.1:29595         127.0.0.1:45868         ESTABLISHED 0          2668
tcp        0      0 127.0.0.1:50206         127.0.0.1:57052         ESTABLISHED 0          4427
tcp        0      0 127.0.0.1:59983         127.0.0.1:42946         ESTABLISHED 0          4440
tcp        0      0 127.0.0.1:45861         127.0.0.1:29595         ESTABLISHED 0          2633
tcp        0      0 127.0.0.1:45837         127.0.0.1:29595         ESTABLISHED 0          1407
tcp        0      0 127.0.0.1:45893         127.0.0.1:29595         ESTABLISHED 0          4401
tcp        0      0 127.0.0.1:44251         127.0.0.1:36455         ESTABLISHED 0          4273
tcp        0      0 127.0.0.1:29595         127.0.0.1:45893         ESTABLISHED 0          4402
tcp        0      0 127.0.0.1:43938         127.0.0.1:44104         ESTABLISHED 0          1410
tcp        0      0 127.0.0.1:44136         127.0.0.1:43938         ESTABLISHED 0          2672
tcp        0      0 127.0.0.1:33197         127.0.0.1:57883         ESTABLISHED 0          4414
tcp        0      0 127.0.0.1:57037         127.0.0.1:50206         ESTABLISHED 0          4262
tcp        0      0 127.0.0.1:52988         127.0.0.1:47257         ESTABLISHED 0          4590
tcp        0      0 127.0.0.1:29595         127.0.0.1:45839         ESTABLISHED 0          1470
tcp        0      0 127.0.0.1:29595         127.0.0.1:48610         ESTABLISHED 0          7097
tcp        0      0 127.0.0.1:53208         127.0.0.1:35345         ESTABLISHED 0          4269
tcp        0      0 127.0.0.1:59949         127.0.0.1:42946         ESTABLISHED 0          2645
tcp        0      0 127.0.0.1:42946         127.0.0.1:59949         ESTABLISHED 0          2646
tcp        0      0 127.0.0.1:29595         127.0.0.1:45847         ESTABLISHED 0          1487
tcp        0      0 127.0.0.1:39517         127.0.0.1:38492         ESTABLISHED 0          2221
tcp        0      0 127.0.0.1:47252         127.0.0.1:52988         ESTABLISHED 0          4434
tcp        0      0 127.0.0.1:36902         127.0.0.1:51222         ESTABLISHED 0          2606
tcp        0      0 127.0.0.1:53512         127.0.0.1:43904         ESTABLISHED 0          67023
tcp        0      0 127.0.0.1:35345         127.0.0.1:53208         ESTABLISHED 0          4268
tcp        0      0 127.0.0.1:50206         127.0.0.1:57057         ESTABLISHED 0          4571
tcp        0      0 127.0.0.1:29595         127.0.0.1:45840         ESTABLISHED 0          1480
tcp        0      0 127.0.0.1:36359         127.0.0.1:50436         ESTABLISHED 11         67115
tcp        0      0 127.0.0.1:45881         127.0.0.1:29595         ESTABLISHED 0          4258
tcp        0      0 127.0.0.1:50206         127.0.0.1:57019         ESTABLISHED 0          2640
tcp        0      0 127.0.0.1:45862         127.0.0.1:29595         ESTABLISHED 0          2634
tcp        0      0 127.0.0.1:44705         127.0.0.1:53512         ESTABLISHED 11         34885
tcp        0      0 127.0.0.1:38492         127.0.0.1:39517         ESTABLISHED 0          2227
tcp        0      0 127.0.0.1:34256         127.0.0.1:55985         ESTABLISHED 0          4278
tcp        0      0 127.0.0.1:45846         127.0.0.1:29595         ESTABLISHED 0          1477
tcp        0      0 127.0.0.1:50206         127.0.0.1:57004         ESTABLISHED 0          2224
tcp        0      0 127.0.0.1:55985         127.0.0.1:34244         ESTABLISHED 0          2687
tcp        0      0 127.0.0.1:57027         127.0.0.1:50206         ESTABLISHED 0          2677
tcp        0      0 127.0.0.1:29595         127.0.0.1:45844         ESTABLISHED 0          1484
```

```
tcp        0      0 127.0.0.1:29595         127.0.0.1:45856         ESTABLISHED 0          2585
tcp        0      0 127.0.0.1:44992         127.0.0.1:36015         ESTABLISHED 11         34890
tcp        0      0 127.0.0.1:56441         127.0.0.1:36773         ESTABLISHED 0          2642
tcp        0      0 127.0.0.1:48610         127.0.0.1:29595         ESTABLISHED 11         7096
tcp        0      0 127.0.0.1:53208         127.0.0.1:35369         ESTABLISHED 0          5131
tcp        0      0 127.0.0.1:41248         127.0.0.1:33775         ESTABLISHED 0          2683
tcp        0      0 127.0.0.1:43906         127.0.0.1:50436         ESTABLISHED 11         7120
tcp        0      0 127.0.0.1:53208         127.0.0.1:35340         ESTABLISHED 0          4260
tcp        0      0 127.0.0.1:50436         127.0.0.1:36359         ESTABLISHED 0          67116
tcp        0      0 127.0.0.1:50206         127.0.0.1:57037         ESTABLISHED 0          4263
tcp        0      0 127.0.0.1:29595         127.0.0.1:45861         ESTABLISHED 0          2636
tcp        0      0 127.0.0.1:36015         127.0.0.1:44992         ESTABLISHED 0          34889
tcp        0      0 127.0.0.1:36455         127.0.0.1:44251         ESTABLISHED 0          4274
tcp        0      0 127.0.0.1:50436         127.0.0.1:59528         ESTABLISHED 0          4577
tcp        0      0 127.0.0.1:57010         127.0.0.1:50206         ESTABLISHED 0          2582
tcp        0      0 127.0.0.1:56564         127.0.0.1:46496         ESTABLISHED 0          2596
tcp        0      0 127.0.0.1:50206         127.0.0.1:57012         ESTABLISHED 0          2594
tcp        0      0 127.0.0.1:36455         127.0.0.1:44239         ESTABLISHED 0          2685
tcp        0      0 127.0.0.1:43938         127.0.0.1:44118         ESTABLISHED 0          2223
tcp        0      0 127.0.0.1:51222         127.0.0.1:36916         ESTABLISHED 0          2681
tcp        0      0 127.0.0.1:35369         127.0.0.1:53208         ESTABLISHED 0          5130
tcp        0      0 127.0.0.1:46496         127.0.0.1:56564         ESTABLISHED 0          2595
tcp        0      0 127.0.0.1:39592         127.0.0.1:46164         ESTABLISHED 0          2689
tcp        0      0 127.0.0.1:50206         127.0.0.1:57039         ESTABLISHED 0          4267
tcp        0      0 127.0.0.1:43279         127.0.0.1:47143         ESTABLISHED 0          4428
tcp        0      0 127.0.0.1:45845         127.0.0.1:29595         ESTABLISHED 0          1476
tcp        0      0 127.0.0.1:43904         127.0.0.1:53512         ESTABLISHED 11         67022
tcp        0      0 127.0.0.1:42946         127.0.0.1:59990         ESTABLISHED 0          5129
tcp        0      0 127.0.0.1:45844         127.0.0.1:29595         ESTABLISHED 0          1475
tcp        0      0 10.10.50.150:22         10.10.50.18:48041       ESTABLISHED 0          34818
tcp        0      0 127.0.0.1:57012         127.0.0.1:50206         ESTABLISHED 0          2593
tcp        0      0 127.0.0.1:51222         127.0.0.1:36902         ESTABLISHED 0          2607
tcp        0      0 127.0.0.1:57008         127.0.0.1:50206         ESTABLISHED 0          2225
tcp        0      0 10.10.50.150:22         10.10.50.16:42536       ESTABLISHED 0          66886
tcp        0      0 127.0.0.1:45860         127.0.0.1:29595         ESTABLISHED 0          2631
tcp        0      0 127.0.0.1:29595         127.0.0.1:45863         ESTABLISHED 0          2638
tcp        0      0 127.0.0.1:44132         127.0.0.1:43938         ESTABLISHED 0          2643
tcp        0      0 127.0.0.1:45868         127.0.0.1:29595         ESTABLISHED 0          2667
tcp        0      0 127.0.0.1:39516         127.0.0.1:38492         ESTABLISHED 0          2220
tcp        0      0 127.0.0.1:29595         127.0.0.1:45842         ESTABLISHED 0          1482
tcp        0      0 127.0.0.1:46164         127.0.0.1:39592         ESTABLISHED 0          2688
tcp        0      0 127.0.0.1:57895         127.0.0.1:33197         ESTABLISHED 0          4596
tcp        0      0 127.0.0.1:44859         127.0.0.1:53512         ESTABLISHED 11         7098
tcp        0      0 127.0.0.1:37210         127.0.0.1:41078         ESTABLISHED 0          4293
tcp        0      0 127.0.0.1:50206         127.0.0.1:57010         ESTABLISHED 0          2583
tcp        0      0 127.0.0.1:53512         127.0.0.1:44859         ESTABLISHED 0          7099
tcp        0      0 127.0.0.1:34260         127.0.0.1:55985         ESTABLISHED 0          4294
tcp        0      0 127.0.0.1:29595         127.0.0.1:45894         ESTABLISHED 0          4415
tcp        0      0 127.0.0.1:57892         127.0.0.1:33197         ESTABLISHED 0          4578
tcp        0      0 127.0.0.1:43938         127.0.0.1:44132         ESTABLISHED 0          2644
tcp        0      0 127.0.0.1:56961         127.0.0.1:34647         ESTABLISHED 11         7103
tcp        0      0 127.0.0.1:43938         127.0.0.1:44136         ESTABLISHED 0          2673
tcp        0      0 127.0.0.1:44086         127.0.0.1:54304         ESTABLISHED 11         67027
tcp        0      0 127.0.0.1:34244         127.0.0.1:55985         ESTABLISHED 0          2686
tcp        0      0 127.0.0.1:57057         127.0.0.1:50206         ESTABLISHED 0          4570
tcp        0      0 127.0.0.1:50436         127.0.0.1:35592         ESTABLISHED 0          35094
tcp        0      0 127.0.0.1:57052         127.0.0.1:50206         ESTABLISHED 0          4426
tcp        0      0 127.0.0.1:59988         127.0.0.1:42946         ESTABLISHED 0          4591
tcp        0      0 127.0.0.1:45836         127.0.0.1:29595         ESTABLISHED 0          1322
tcp        0      0 127.0.0.1:45843         127.0.0.1:29595         ESTABLISHED 0          1474
tcp        0      0 127.0.0.1:45842         127.0.0.1:29595         ESTABLISHED 0          1473
tcp        0      0 127.0.0.1:33197         127.0.0.1:57895         ESTABLISHED 0          4597
tcp        0      0 127.0.0.1:52988         127.0.0.1:47252         ESTABLISHED 0          4435
tcp        0      0 127.0.0.1:53512         127.0.0.1:44705         ESTABLISHED 0          34886
tcp        0      0 127.0.0.1:45840         127.0.0.1:29595         ESTABLISHED 0          1471
tcp        0      0 127.0.0.1:50206         127.0.0.1:57008         ESTABLISHED 0          2228
tcp        0      0 127.0.0.1:33787         127.0.0.1:41248         ESTABLISHED 0          4270
tcp        0      0 127.0.0.1:29595         127.0.0.1:45846         ESTABLISHED 0          1486
tcp        0      0 127.0.0.1:45879         127.0.0.1:29595         ESTABLISHED 0          4253
 --More--
```

run show system core-dumps

The **run show system core-dumps** command displays information about the system core files.

Command Syntax
run show system core-dumps

Example
• This example demonstrates how to show system core-dumps:

```
admin@XorPlus# run show system core-dumps
total 0
```

run show system cpu-usage

The **run show system cpu-usage** command displays information about the cpu usage.

Command Syntax
run show system cpu-usage

Example
• This example demonstrates how to show system connections:

```
admin@XorPlus# run show system cpu-usage
CPU usage: 7%
```

run show system date

The **run show system date** command displays information about the system current date.

Command Syntax
run show system date

Example
• This example demonstrates how to show system date:

```
admin@XorPlus# run show system date
Thu Nov 10 23:55:38 UTC 2005
```

run show system fan

The **run show system fan** command displays information about the system status of fan.

Command Syntax
run show system fan

Example
• This example demonstrates how to show system fan:

```
admin@XorPlus# run show system fan
Sensor Temperature:
Sensor 1 Temperature : 45 C / 113.00 F
Sensor 2 Temperature : 42 C / 107.60 F
Sensor 3 Temperature : 47 C / 116.60 F
Sensor 4 Temperature : 38 C / 100.40 F
Fan Status:
Fan 1 speed = 9747 RPM, PWM = 59, Forward
Fan 2 speed = 9836 RPM, PWM = 59, Forward
Fan 3 speed = 9782 RPM, PWM = 59, Forward
```

run show system memory-usage

The **run show system memory-usage** command displays information about memory usage.

Command Syntax
run show system memory-usage

Example
• This example demonstrates how to show system memory-usage:

```
admin@XorPlus# run show system memory-usage
total used free shared buffers cached
Mem: 515808 200528 315280 0 3048 60864
-/+ buffers/cache: 136616 379192
Swap: 0 0 0
```

run show system name

The **run show system name** command displays information about the host name.

Command Syntax
run show system name

Example
• This example demonstrates how to show system name:

```
admin@XorPlus# run show system name
admin@XorPlus
```

run show system ntp-status

The **run show system ntp-status** command displays information about the switch NTP status.

Command Syntax
run show system ntp-status

Example
• This example demonstrates how to show system ntp-status:

```
admin@XorPlus# run show system ntp-status
NTP Server information:
server 192.168.10.100
NTP Server Sync information:
ntp_gettime() returns code 0 (OK)
  time d709f74e.9b523000  Tue, Apr 29 2014 10:02:54.606, (.606723),
  maximum error 6016 us, estimated error 16 us, TAI offset 0
ntp_adjtime() returns code 0 (OK)
  modes 0x0 (),
  offset 0.000 us, frequency 0.000 ppm, interval 1 s,
  maximum error 6016 us, estimated error 16 us,
  status 0x1 (PLL),
  time constant 7, precision 1.000 us, tolerance 500 ppm,
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 192.168.10.100  .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

run show system os

The **run show system os** command displays information about operating system details.

Command Syntax
run show system os

Example
• This example demonstrates how to show system os:

```
admin@XorPlus# run show system os
Linux XorPlus 2.6.27 #1 Mon Mar 3 20:40:05 CST 2014 ppc GNU/Linux
```

run show system processes brief

The **run show system processes brief** command displays processes in a brief format.

Command Syntax
run show system processes brief

Example
• This example demonstrates how to show system processes succinctly:

```
admin@XorPlus# run show system processes brief
PID TTY STAT TIME COMMAND
1 ? Ss 0:01 init [2]
2 ? S< 0:00 [kthreadd]
3 ? S< 0:01 [ksoftirqd/0]
4 ? S< 0:00 [watchdog/0]
5 ? S< 0:14 [events/0]
6 ? S< 0:00 [khelper]
48 ? S< 0:00 [kblockd/0]
55 ? S< 0:00 [ata/0]
56 ? S< 0:00 [ata_aux]
58 ? S< 0:00 [kseriod]
99 ? S 0:00 [pdflush]
100 ? S 0:00 [pdflush]
101 ? S< 0:00 [kswapd0]
147 ? S< 0:00 [aio/0]
156 ? S< 0:00 [nfsiod]
831 ? S< 0:00 [ftld]
853 ? S< 0:00 [rpciod/0]
857 ? S< 0:00 [kjournald]
2338 ? Ss 0:00 /usr/sbin/cron -L 0
2370 ? Ss 0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6
2483 ? S 0:18 pica_cardmgr
2485 ? S 6:14 pica_sif
2631 ? S 0:32 pica_lacp
2648 ? Sl 102:22 pica_lcmgr
2654 ? S 0:29 pica_login
3405 ? S 3:10 pica_mstp
3409 ? S 0:18 xorp_policy
3411 ? Ss 8:12 /pica/bin/xorp_rtrmgr -d -L local0.info -P /var/run/xorp_rtrmgr.pid
3450 ? S 0:57 pica_dhcp
3466 ? S 0:36 xorp_static_routes
3474 ? S 0:37 xorp_ospfv2
3511 tty1 Ss+ 0:00 /sbin/getty 38400 tty1
3518 tty2 Ss+ 0:00 /sbin/getty 38400 tty2
3519 tty3 Ss+ 0:00 /sbin/getty 38400 tty3
3816 ? Ss 0:00 dhclient eth0
4880 ? Ss 0:00 in.telnetd: 10.10.50.47
4881 pts/0 Ss 0:00 login -h 10.10.50.47 -p
4882 pts/0 S+ 0:00 -bash
4891 pts/0 S+ 0:02 /pica/bin/pica_sh
9021 pts/0 R 0:00 ps ax
15109 ? Ss 0:00 in.telnetd: 10.10.50.47
15110 pts/1 Ss 0:00 login -h 10.10.50.47 -p
15111 pts/1 S+ 0:00 -bash
15120 pts/1 S+ 0:17 /pica/bin/pica_sh
15327 ? Ss 0:00 in.telnetd: 10.10.50.47
15328 pts/2 Ss 0:00 login -h 10.10.50.47 -p
15342 pts/2 S+ 0:00 -bash
15351 pts/2 S+ 0:26 /pica/bin/pica_sh
15869 ttyS0 Ss 0:00 /bin/login -
```

```
15870 ttyS0 S+ 0:00 -bash
15881 ttyS0 S+ 0:17 /pica/bin/pica_sh
21746 ? Ss 0:00 in.telnetd: 10.10.50.153
21747 pts/3 Ss 0:00 login -h 10.10.50.153 -p
21748 pts/3 S+ 0:00 -bash
21757 pts/3 S+ 0:10 /pica/bin/pica_sh
27523 ? Sl 0:00 /usr/sbin/rsyslogd -c5
31989 ? S 0:00 radvd
31990 ? Ss 0:01 radvd
```

run show system processes detail

The **run show system processes detail** command displays processes in a detailed format.

Command Syntax
run show system processes detail

Example
• This example demonstrates how to show system processes detail:

```
admin@XorPlus# run show system processes detail
USER   PID   %CPU   %MEM   VSZ   RSS   TTY   STAT  START   TIME    COMMAND
root   1      0.0   0.1   2400   856    ?     Ss   Nov09   0:01    init [2]
root   2      0.0   0.0    0      0     ?     S<   Nov09   0:00   [kthreadd]
root   3      0.0   0.0    0      0     ?     S<   Nov09   0:01   [ksoftirqd/0]
root   4      0.0   0.0    0      0     ?     S<   Nov09   0:00   [watchdog/0]
root   5      0.0   0.0    0      0     ?     S<   Nov09   0:14   [events/0]
root   6      0.0   0.0    0      0     ?     S<   Nov09   0:00   [khelper]
root   48     0.0   0.0    0      0     ?     S<   Nov09   0:00   [kblockd/0]
root   55     0.0   0.0    0      0     ?     S<   Nov09   0:00   [ata/0]
root   56     0.0   0.0    0      0     ?     S<   Nov09   0:00   [ata_aux]
root   58     0.0   0.0    0      0     ?     S<   Nov09   0:00   [kseriod]
root   99     0.0   0.0    0      0     ?     S    Nov09   0:00   [pdflush]
root   100    0.0   0.0    0      0     ?     S    Nov09   0:00   [pdflush]
root   101    0.0   0.0    0      0     ?     S<   Nov09   0:00   [kswapd0]
root   147    0.0   0.0    0      0     ?     S<   Nov09   0:00   [aio/0]
root   156    0.0   0.0    0      0     ?     S<   Nov09   0:00   [nfsiod]
root   831    0.0   0.0    0      0     ?     S<   Nov09   0:00   [ftld]
root   853    0.0   0.0    0      0     ?     S<   Nov09   0:00   [rpciod/0]
root   857    0.0   0.0    0      0     ?     S<   Nov09   0:00   [kjournald]
root   2338   0.0   0.1   2768   852    ?     Ss   Nov09   0:00   /usr/sbin/cron -L 0
root   2370   0.0   0.1   3656   1020   ?     Ss   Nov09   0:00   /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -st
root   2483   0.0   1.4   22660  7532   ?     S    Nov09   0:18   pica_cardmgr
root   2485   0.4   4.5   43000  23444  ?     S    Nov09   6:16   pica_sif
root   2631   0.0   1.6   26504  8620   ?     S    Nov09   0:32   pica_lacp
root   2648   6.6   5.6   108136 29188  ?     Sl   Nov09   103:00 pica_lcmgr
root   2654   0.0   2.4   30596  12688  ?     S    Nov09   0:30   pica_login
root   3405   0.2   2.7   32244  14200  ?     S    Nov09   3:11   pica_mstp
root   3409   0.0   1.3   18624  7100   ?     S    Nov09   0:18   xorp_policy
root   3411   0.5   3.4   40304  17772  ?     Ss   Nov09   8:16   /pica/bin/xorp_rtrmgr -d -L local0.info -P /var/r
root   3450   0.0   1.8   27524  9488   ?     S    Nov09   0:58   pica_dhcp
root   3466   0.0   1.4   18060  7284   ?     S    Nov09   0:36   xorp_static_routes
root   3474   0.0   1.4   19816  7600   ?     S    Nov09   0:37   xorp_ospfv2
root   3511   0.0   0.1   2672   916   tty1   Ss+  Nov09   0:00   /sbin/getty 38400 tty1
root   3518   0.0   0.1   2672   916   tty2   Ss+  Nov09   0:00   /sbin/getty 38400 tty2
root   3519   0.0   0.1   2672   916   tty3   Ss+  Nov09   0:00   /sbin/getty 38400 tty3
root   3816   0.0   0.4   5128   2336   ?     Ss   Nov09   0:00   dhclient eth0
root   4880   0.0   0.2   2784   1084   ?     Ss   Nov10   0:00   in.telnetd: 10.10.50.47
root   4881   0.0   0.2   3492   1268  pts/0  Ss   Nov10   0:00   login -h 10.10.50.47 -p
admin  4882   0.0   0.2   3500   1544  pts/0  S+   Nov10   0:00   -bash
admin  4891   0.0   2.1   38396  11308 pts/0  S+   Nov10   0:02   /pica/bin/pica_sh
admin  9436   0.0   0.2   3208   1112  pts/0  R    00:31   0:00   ps aux
root   15109  0.0   0.2   2784   1084   ?     Ss   Nov10   0:00   in.telnetd: 10.10.50.47
root   15110  0.0   0.2   3492   1268  pts/1  Ss   Nov10   0:00   login -h 10.10.50.47 -p
admin  15111  0.0   0.2   3500   1544  pts/1  S+   Nov10   0:00   -bash
admin  15120  0.0   2.4   40068  12536 pts/1  S+   Nov10   0:17   /pica/bin/pica_sh
root   15327  0.0   0.2   2784   1092   ?     Ss   Nov10   0:00   in.telnetd: 10.10.50.47
root   15328  0.0   0.2   3492   1268  pts/2  Ss   Nov10   0:00   login -h 10.10.50.47 -p
admin  15342  0.0   0.2   3500   1544  pts/2  S+   Nov10   0:00   -bash
admin  15351  0.0   2.6   41480  13684 pts/2  S+   Nov10   0:27   /pica/bin/pica_sh
root   15869  0.0   0.2   3492   1268  ttyS0  Ss   Nov10   0:00   /bin/login -
```

```
admin  15870  0.0   0.3   3540   1696  ttyS0  S+   Nov10   0:00   -bash
admin  15881  0.0   2.6   41272  13908 ttyS0  S+   Nov10   0:17   /pica/bin/pica_sh
root   21746  0.0   0.2   2784   1084    ?    Ss   Nov10   0:00   in.telnetd: 10.10.50.153
root   21747  0.0   0.2   1268          pts/3  Ss   Nov10   0:00   login -h 10.10.50.153 -p
admin  21748  0.0   0.2   3500   1544  pts/3  S+   Nov10   0:00   -bash
admin  21757  0.0   2.2   39704  11652 pts/3  S+   Nov10   0:10   /pica/bin/pica_sh
root   27523  0.0   0.3   28488  1736   ?     Sl   Nov10   0:00   /usr/sbin/rsyslogd -c5
root   31989  0.0   0.0   2448   368    ?     S    Nov10   0:00   radvd
root   31990  0.0   0.0   2448   508    ?     Ss   Nov10   0:01   radvd
```

run show system rollback compare to

The **run show system rollback compare to** command shows the difference between tow rolled back configurations.

Command Syntax
run show system rollback compare to <other-config>

Parameter
•<other-config>Show the difference between rolled back configuration [1-49] and current configuration.

Example
• This example demonstrates how to show system rollback compare to 02:

```
admin@XorPlus# run show system rollback compare to 02
3c3
< /*Last commit     : Tue Apr 29 10:02:42 2014 by admin*/
---
> /*Last commit     : Tue Apr 29 09:38:47 2014 by admin*/
23c23
<             code-point 32
---
>             code-point 0
1254d1253
<     ntp-server-ip 192.168.10.100
```

run show system rollback file

The **run show system rollback file** command shows rolled back configuration file.

Command Syntax
run show system rollback file <rollback>

Parameter
•<other-config>Show rolled back configuration, range is [01, 02, 03, ... 49].

Example
• This example demonstrates how to show system rollback file 01:

```
admin@XorPlus# run show system rollback file 01
/*XORP Configuration File, v1.0*/
/* Copyright (C) 2009-2013 Pica8, Inc.*/
/*Last commit     : Fri Nov 11 15:17:55 2005 by root*/
/*PicOS Version   : 2.0.6*/
/*Version Checksum: 6165f4a04921d24410b9bf2780b0a960*/
interface {
    ecmp {
        max-path: 4
        hash-mapping {
            field {
                ingress-interface {
                    disable: true
                }
                vlan {
                    disable: true
                }
                ip-protocol {
                    disable: true
                }
                ip-source {
                    disable: false
                }
                ip-destination {
                    disable: false
                }
                port-source {
                    disable: false
                }
                port-destination {
                    disable: false
                }
            }
        }
    }
    aggregate-balancing {
        hash-mapping {
            field {
                ingress-interface {
                    disable: false
                }
                ethernet-source-address {
                    disable: false
                }
                ethernet-destination-address {
                    disable: false
                }
                ethernet-type {
```

```
                disable: false
            }
            vlan {
                disable: false
            }
            ip-protocol {
                disable: false
            }
            ip-source {
                disable: false
            }
            ip-destination {
                disable: false
            }
            port-source {
                disable: false
            }
            port-destination {
                disable: false
            }
--More--
```

run show system rollback list

The **run show system rollback list** command shows rolled back file list.

Command Syntax
run show system rollback list

Example
• This example demonstrates how to show system rollback list:

```
admin@XorPlus# run show system rollback list
-rw-rw-r-- 1 admin xorp 14003 Nov 11 15:43 /pica/config/pica.conf
-rw-rw-r-- 1 admin xorp 14003 Nov 11 15:42 /pica/config/pica.conf.01
-rw-rw-r-- 1 root  xorp 13878 Nov 11 15:17 /pica/config/pica.conf.02
```

run show system rpsu

The **run show system rpsu** command shows the status of Redundant Power Supply Unit.

Command Syntax
run show system rpsu

Example
• This example demonstrates how to show system rpsu:

```
admin@XorPlus# run show system rpsu
RPSU is not supported for Pronto3290
```

run show system serial-number

The **run show system serial-number** command shows the serial number of Motherboard, RPSU, and SFP module.

Command Syntax
run show system serial-number

Example
• This example demonstrates how to show system serial-number:

```
admin@XorPlus# run show system serial-number

MotherBoard Serial Number : TW0WYGRVDNT0097I0015

RPSU 1 Serial Number      : N/A
RPSU 2: Not ready
SFP+    te-1/1/49             :
        Vendor Name           : Hisense
        Vendor PartNr         : LTF8502-BC+
        Serial Number         : CN56GMC2S0
        Module Type           : 10G_BASE_SR
        Cable Length          : 300m
SFP     te-1/1/50             :
        Vendor Name           : FiberStore
        Vendor PartNr         : SFP1G-LX-31
        Serial Number         : F174CO01408
        Module Type           : 1G_BASE_LX
        Cable Length          : 10km
SFP     te-1/1/51             :
        Vendor Name           : FiberStore
        Vendor PartNr         : SFP1G-LX-31
        Serial Number         : F174CO01641
        Module Type           : 1G_BASE_LX
        Cable Length          : 10km
SFP+    te-1/1/52             :
        Vendor Name           : 3M
        Vendor PartNr         : 1410-P17-00-3.00
        Serial Number         : Y30B220863
        Module Type           : 10G_BASE_AOC
        Cable Length          : 30m
```

run show system temperature

The **run show system temperature** command shows the switch temperature.

Command Syntax
run show system temperature

Example
• This example demonstrates how to show system temperature:

```
admin@XorPlus# run show system temperature
Temperature: 41 C / 105 F
```

run show system uptime

The **run show system uptime** command shows the time since system and processes started.

Command Syntax
run show system uptime

Example
• This example demonstrates how to show system uptime:

```
admin@XorPlus# run show system uptime
16:01:44 up 53 min, 3 users, load average: 0.09, 0.07, 0.09
```

run show system users

The **run show system users** command shows users who are currently logging in.

Command Syntax
run show system users

Example
• This example demonstrates how to show system users:

```
admin@XorPlus# run show system users
admin pts/0 Nov 11 15:35 (10.10.50.47)
admin ttyS0 Nov 11 15:18
admin pts/1 Nov 11 15:38 (10.10.50.47)
```

set system aaa local disable

The **set system aaa local disable** command enables the local authentication function.

Command Syntax
set system aaa local disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the local authentication function. The value is **true** or **false**. **true**: disables the local authentication function. **false**: enables the local authentication function. The default value is **false**.

Example
• Enable the local authentication function.

```
admin@XorPlus# set system aaa local disable true
admin@XorPlus# commit
```

set system aaa radius accounting disable

The **set system aaa radius accounting disable** command enables the RADIUS accounting function.

Command Syntax
set system aaa radius accounting disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the RADIUS accounting function. The value is **true** or **false**. **true**: disables the RADIUS accounting function. **false**: enables the RADIUS accounting function. The default value is **true**.

Example

• Enable the RADIUS accounting function.

```
admin@XorPlus# set system aaa radius accounting disable false
admin@XorPlus# commit
```

set system aaa radius accounting server-ip

The **set system aaa radius accounting server-ip** command configures IP address of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip <*ip_address*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.

Example
- Configure IP address of a RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41
admin@XorPlus# commit
```

set system aaa radius accounting server-ip port

The **set system aaa radius accounting server-ip port** command configures port number of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip *<ip_address>* **port** *<integer>*

Parameter

Parameter	Description
server-ip *<ip_address>*	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.
port *<integer>*	Specifies a port of a RADIUS accounting server. The value is an integer type. The default value is 1812. Note: The value of port number should be the same with that on the RADIUS servers.

Example
•Configure the port number of a RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41 port 2
admin@XorPlus# commit
```

set system aaa radius accounting server-ip shared-key

The **set system aaa radius accounting server-ip shared-key** command configures shared key of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip <*ip_address*> **shared-key** <*string*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.
shared-key <*string*>	Specifies the shared key of RADIUS accounting server. The value is a string type. Note: The value of shared key should be the same with that on the RADIUS accounting servers.

Example
• Configure the shared key of RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41 shared-key test123
admin@XorPlus# commit
```

set system aaa radius accounting server-ip timeout

The **set system aaa radius accounting server-ip timeout** command configures the response timeout interval of a RADIUS accounting server.

Command Syntax
set system aaa radius accounting server-ip <*ip_address*> **timeout** <*integer*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS accounting server. The value could be an IPv4 or IPv6 address.
timeout <*integer*>	Specifies the response timeout interval of a RADIUS accounting server. When the NAS server sends a request message to the RADIUS accounting server, it considers the server is inactive if it receives no response message from the server within the specified time. The value is an integer in seconds. The default value is 5s.

Example
• Configure the response timeout interval of a RADIUS accounting server.

```
admin@XorPlus# set system aaa radius accounting server-ip 10.10.50.41 timeout 5
admin@XorPlus# commit
```

set system aaa radius authorization disable

The **set system aaa radius authorization disable** command enables the RADIUS authentication and authorization function.

Command Syntax
set system aaa radius authorization disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the RADIUS authentication and authorization function. The value is **true** or **false**. **true**: disables the RADIUS authentication and authorization function. **false**: enables the RADIUS authentication and authorization function. The default value is **true**.

Example
- Enable the RADIUS authentication and authorization function.

```
admin@XorPlus# set system aaa radius authorization disable false
admin@XorPlus# commit
```

set system aaa radius authorization server-ip

The **set system aaa radius authorization server-ip** command configures IP address of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.

Example
- Configure IP address of a RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41
admin@XorPlus# commit
```

set system aaa radius authorization server-ip port

The **set system aaa radius authorization server-ip port** command configures port number of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*> **port** <*integer*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies the IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.
port <*integer*>	Specifies a port of a RADIUS authentication and authorization server. The value is an integer type. The default value is 1812. Note: The value of port number should be the same with that on the RADIUS servers.

Example
- Configure the port number of a RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41 port 2
admin@XorPlus# commit
```

set system aaa radius authorization server-ip shared-key

The **set system aaa radius authorization server-ip shared-key** command configures shared-key of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*> **shared-key** <*string*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.
shared-key <*string*>	Specifies the shared key of RADIUS authentication and authorization server. The value is a string type. Note: The value of shared key should be the same with that on the RADIUS servers.

Example
• Configure the shared key of RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41 shared-key test123
admin@XorPlus# commit
```

set system aaa radius authorization server-ip timeout

The **set system aaa radius authorization server-ip timeout** command configures the response timeout interval of a RADIUS authentication and authorization server.

Command Syntax
set system aaa radius authorization server-ip <*ip_address*> **timeout** <*integer*>

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of RADIUS authentication and authorization server. The value could be an IPv4 or IPv6 address.
timeout <*integer*>	Specifies the response timeout interval of a RADIUS authentication and authorization server. When the NAS server sends a request message to the RADIUS authentication and authorization server, it considers the server is inactive if it receives no response message from the server within the specified time. The value is an integer in seconds. The default value is 5s.

Example
- Configure the response timeout interval of a RADIUS authentication and authorization server.

```
admin@XorPlus# set system aaa radius authorization server-ip 10.10.50.41 timeout 5
admin@XorPlus# commit
```

set system aaa radius vrf mgmt-vrf

The **set system aaa radius vrf mgmt-vrf** command configures to run the AAA RADIUS protocol in management VRF.

Command Syntax

set system aaa radius vrf mgmt-vrf

Parameter

None.

Usage Guidelines

AAA RADIUS protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding AAA server is required to be route reachable in the VRF running AAA RADIUS protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the AAA RADIUS protocol to run in the management VRF.

```
admin@Xorplus# set system aaa radius vrf mgmt-vrf
admin@Xorplus# commit
```

set system aaa tacacs-plus accounting

The **set system aaa tacacs-plus accounting** command enables the TACACS+ accounting function.

Command Syntax
set system aaa tacacs-plus accounting <true | false>

Parameter

Parameter	Description
accounting <true | false>	Configures whether to enable or disable the TACACS+ accounting function. The value is **true** or **false**. **true**: enables the TACACS+ accounting function. It will take effect only when the TACACS+ function is enabled. **false**: disables the TACACS+ accounting function. The default value is **true**.

Example
- Enable the TACACS+ accounting function.

```
admin@XorPlus# set system aaa tacacs-plus accounting true
admin@XorPlus# commit
```

set system aaa tacacs-plus authorization

The **set system aaa tacacs-plus authorization** command enables the TACACS+ authorization function.

Command Syntax

set system aaa tacacs-plus authorization <**true | false**>

Parameter

Parameter	Description
authorization <true | false>	Configures whether to enable or disable the TACACS+ authorization function. The value is **true** or **false**. **true**: enables the TACACS+ authorization function. It will take effect only when the TACACS+ function is enabled. **false**: disables the TACACS+ authorization function. The default value is **true**.

Example

- Enable the TACACS+ authorization function.

```
admin@XorPlus# set system aaa tacacs-plus authorization true
admin@XorPlus# commit
```

set system aaa tacacs-plus auth-type

The **set system aaa tacacs-plus auth-type** command configures TACACS+ authentication type.

Command Syntax
set system aaa tacacs-plus auth-type <**ascii** | **chap** | **pap**>

Parameter

Parameter	Description
auth-type <ascii | chap | pap>	Specifies TACACS+ authentication type. The value could be **ascii**, **chap** or **pap**. The default value is **ascii**.

Example
- Configure TACACS+ authentication type.

```
admin@XorPlus# set system aaa tacacs-plus auth-type ascii
admin@XorPlus# commit
```

set system aaa tacacs-plus disable

The **set system aaa tacacs-plus disable** command enables the TACACS+ function.

Command Syntax

set system aaa tacacs-plus disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Configures whether to enable or disable the TACACS+ function. The value is **true** or **false**. **true**: disables the TACACS+ function. **false**: enables the TACACS+ function. The default value is **true**.

Example

- Enable the TACACS+ function.

```
admin@XorPlus# set system aaa tacacs-plus disable false
admin@XorPlus# commit
```

set system aaa tacacs-plus key

The **set system aaa tacacs-plus key** command configures the shared key of TACACS+ server.

Command Syntax

set system aaa tacacs-plus key <*string*>

Parameter

Parameter	Description
key <*string*>	Specifies the shared key of TACACS+ server. The value is a string type. The default value is keystring. Note: The value of shared key should be the same with that on the TACACS+ servers.

Example

- Configure the shared key of TACACS+ server.

```
admin@XorPlus# set system aaa tacacs-plus key pica8pica8
admin@XorPlus# commit
```

set system aaa tacacs-plus port-number

The **set system aaa tacacs-plus port-number** command configures the port number of a TACACS+ server.

Command Syntax
set system aaa tacacs-plus port-number <*integer*>

Parameter

Parameter	Description
port-number <*integer*>	Specifies a port of a TACACS+ server. The value is an integer type. The default value is 49. Note: The value of port number should be the same with that on the TACACS+ servers.

Example
- Configure the port number of a TACACS+ server.

```
admin@XorPlus# set system aaa tacacs-plus port-number 3
admin@XorPlus# commit
```

set system aaa tacacs-plus timeout

The **set system aaa tacacs-plus timeout** command configures the response timeout interval of a TACACS+ server.

Command Syntax

set system aaa tacacs-plus timeout *<integer>*

Parameters

Parameter	Description
timeout *<integer>*	Specifies the response timeout interval of a TACACS+ server. When the NAS server sends a request message to the TACACS+ server, it considers the server is inactive if it receives no response message from the server within the specified time. The value is an integer in seconds. The default value is 5s.

Example

- Configure the response timeout interval of a TACACS+ server.

```
admin@Xorplus# set system aaa tacacs-plus timeout 30
```

set system aaa tacacs-plus server-ip

The **set system aaa tacacs-plus server-ip** command configures IP address of a TACACS+ server.

Command Syntax
set system aaa tacacs-plus server-ip <*ipv4_address*>

Parameter

Parameter	Description
server-ip <*ipv4_address*>	Specifies IP address of a TACACS+ server. The value is in dotted decimal notation.

Usage Guidelines

PicOS supports a maximum of eight TACACS+ servers. When multiple TACACS+ servers are configured, only one will be used, the IP addresses are used in alphabetical order.

For example, the following TACACS+ servers are configured.

```
set system aaa tacacs-plus server-ip 146.13.191.77
set system aaa tacacs-plus server-ip 146.13.191.78
set system aaa tacacs-plus server-ip 1.1.1.1
set system aaa tacacs-plus server-ip 2.2.2.2
set system aaa tacacs-plus server-ip 3.3.3.3
```

The servers will be used in below order.

1. 1.1.1.1
2. 146.13.191.77
3. 146.13.191.78
4. 2.2.2.2
5. 3.3.3.3

Example
- Configure IP address of a TACACS+ server.

```
admin@XorPlus# set system aaa tacacs-plus server-ip 10.10.53.53
admin@XorPlus# commit
```

set system aaa tacacs-plus source-interface

The **set system aaa tacacs-plus source-interface** command sets the source interface the switch uses to connect to the TACACS+ server.

Command Syntax

set system aaa tacacs-plus source-interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the source interface. The value could be an L3 VLAN interface, loopback interface, routed interface or sub-interface that enabled inband management or eth0. By default, the source interface is eth0.

Usage Guidelines

NOTE:

- When using a L3 VLAN interface, loopback interface, routed interface or sub-interface as a source interface connecting to the TACACS+ server, you have to enable inband management function by using commands **set system inband vlan-interface** <*vlan-interface*>, **set system inband loopback** <*loopback-interface*>, **set system inband routed-interface** <*routed-interface*>.
- Remember to specify an IP address for the source interface.

Example

- Set the source interface the switch uses to connect to the server to loopback interface.

```
admin@Xorplus# set l3-interface loopback lo address 10.1.1.1 prefix-length 32
admin@Xorplus# set system aaa tacacs-plus source-interface loopback
```

- Set the source interface the switch uses to connect to the server to L3 VLAN interface.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching native-vlan-id 100
admin@Xorplus# set l3-interface vlan-interface vlan100 address 10.10.51.129 prefix-length 24
admin@Xorplus# set vlans vlan-id 100 l3-interface vlan100
admin@Xorplus# set system inband vlan-interface vlan100
admin@Xorplus# set system aaa tacacs-plus source-interface vlan100
```

set system aaa local-auth-fallback disable

The **set system aaa local-auth-fallback disable** command is used to enable or disable the local authentication fallback function.

Command Syntax

set system aaa local-auth-fallback disable <true | false>

Parameter

Parameter	Description
disable <true | false>	Enable or disable the local authentication fallback function. The value could be **true** or **false**. • **true**: disables the local authentication fallback function. • **false**: enables the local authentication fallback function. By default, the local authentication fallback function is disabled.

Usage Guidelines

For management port or in-band interface login, if the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available, the system determines whether to perform local authentication based on the configuration of local authentication fallback function,

- If the local authentication fallback function is enabled, then user will fallback to local authentication.
- If the local authentication fallback function is disabled, then the system generates a syslog message and user is denied access to local authentication.

NOTE:

- The local authentication fallback function is only applied to management port or in-band login interface in situations where the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available.
- The **set system aaa local-auth-fallback disable <true | false>** command does not applied to console login. For console login, if the TACACS+/RADIUS server is unreachable or the TACACS+/RADIUS service is not available, the system generates a syslog and uses local user/passwd file for authentication. After successful login, local authorization will be performed.

Example

- Enable local authentication fallback function.

```
admin@Xorplus# set system aaa local-auth-fallback disable false
admin@Xorplus# commit
```

set system aaa tacacs-plus vrf mgmt-vrf

The **set system aaa tacacs-plus vrf mgmt-vrf** command configures to run the AAA TACACS+ protocol in management VRF.

Command Syntax

set system tacacs-plus radius vrf mgmt-vrf

Parameter

None.

Usage Guidelines

AAA TACACS+ protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding AAA server is required to be route reachable in the VRF running AAA TACACS+ protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the AAA TACACS+ protocol to run in the management VRF.

```
admin@Xorplus# set system aaa radius vrf mgmt-vrf
admin@Xorplus# commit
```

set system hostname

To specify or modify the hostname for the switch, use the **set system hostname** command in L2/L3 configuration mode. To reset the hostname to default, use the **delete** form of this command.

Command Syntax

set system hostname *hostname*
delete system hostname

Parameters

hostname	New hostname for the switch. The maximum length is 63.

Example

This example demonstrates how to configure the system's network name to 123.

```
admin@Switch# set system hostname 123
admin@Switch# commit
Commit OK.
Save done.
admin@123#
```

set system inband vlan-interface

The **set system inband vlan-interface** command sets a specified L3 VLAN interface in the default VRF as the inband management port.

Command Syntax

set system inband vlan-interface <*vlan-interface*>

Parameter

Parameter	Description
vlan-interface <*vlan-interface*>	Enables inband management on a specfied L3 VLAN interface in the default VRF. The value is a string.

Usage Guidelines

By default, the user cannot remotely log in and manage the switch through the L3 VLAN interface.

Use this command to set a specified L3 VLAN interface in the default VRF as the inband management port. The L3 VLAN interface with the inband management function enabled can transmit both management traffic and data plane traffic.

NOTE:

Only the L3 VLAN interface in the default VRF can be set as the inband management port. If a VLAN interface has been set as an inband management port, it cannot be bound to other user-defined VRFs.

Example

- Enable the inband management function of the L3 VLAN interface vlan100.

```
admin@Xorplus# set system inband vlan-interface vlan100
admin@Xorplus# commit
```

set system inband loopback

The **set system inband loopback** command sets the loopback interface IP in the default VRF as the inband management IP.

Command Syntax

set system inband loopback <*ip-address*>

Parameter

Parameter	Description
loopback <*ip-address*>	Specifies the loopback interface IP in the default VRF as the inband management IP. The value could be an IPv4 or IPv6 address.

Example

- Enable the inband management function of the loopback interface.

```
admin@Xorplus# set system inband loopback 192.168.100.1
admin@Xorplus# commit
```

set system inband routed-interface

The **set system inband routed-interface** command sets a specified routed interface or sub-interface in the default VRF as the inband management port.

Command Syntax

set system inband routed-interface <*routed-interface*>

Parameter

Parameter	Description
routed-interface <*routed-interface*>	Enables inband management on a specfied routed interface or sub-interface in the default VRF. The value is a string.

Usage Guidelines

By default, the user cannot remotely log in and manage the switch through the routed interface or sub-interface.

Use this command to set a specified routed interface or sub-interface in the default VRF as the inband management port. The routed interface or sub-interface with the inband management function enabled can transmit both management traffic and data plane traffic.

NOTE:

Only the routed interface or sub-interface in the default VRF can be set as the inband management port. If a routed interface or sub-interface has been set as an inband management port, it cannot be bound to other user-defined VRFs.

Example

- Enable the inband management function of the routed interface.

```
admin@Xorplus# set system inband routed-interface rif-te1
admin@Xorplus# commit
```

set system inband enable

Warning:
The command **set system inband enable true** is obsolete and replaced by command **set system inband vlan-interface** <*vlan-interface*>, **set system inband loopback** <*loopback-interface*>, **set system inband routed-interface** <*routed-interface*>.

The **set system inband enable** command is used to enable or disable the inband management function for all the L3 interfaces in the default VRF.

Command Syntax

set system inband enable <**true | false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enables or disables the inband management function for all the L3 interfaces in the default VRF. The value could be **true** or **false**. • **true**: enables the inband management function for all the L3 interfaces in the default VRF. • **false**: disables the inband management function for all the L3 interfaces in the default VRF. By default, inband management function is disabled.

Example

- Enable the inband management function for all the L3 interfaces in the default VRF.

```
admin@XorPlus# set system inband enable true
admin@XorPlus# commit
```

system login-acl network

User can configure the ACL to control whether remote hosts within specified subnetworks are allowed to log in the system. User can set ipv4-address/netmask or ipv6-address/netmask to configure remote hosts from both subnetworks log in. User can also delete them.

Command Syntax
set system login-acl network <*IPV4Net*>
set system login-acl network <*IPV6Net*>
delete system login-acl network <*IPV4Net*>
delete system login-acl network <*IPV6Net*>

Parameter
• <*IPV4Net*> It stands ipv4 address and netmask.
• <*IPV6Net*> It stands ipv6 address and netmask.

Example
• This example demonstrates how to configure the login ACL attributes is ipv4-address and netmask:

```
admin@XorPlus# set system login-acl network 192.168.1.0/24
admin@XorPlus# commit
```

• This example demonstrates how to configure the login ACL attributes is ipv6-address and netmask:

```
admin@XorPlus# set system login-acl network 2001:1:1:1::/64
admin@XorPlus# commit
```

system login announcement

User can configure a system announcement message (displayed after login).

Command Syntax
set system login announcement <*text*>
delete system login announcement

Parameter
• <*text*> VLAN tag identifier. The effective value type is text.

Example
• This example demonstrates how to configure the system announcement message after login:

```
admin@XorPlus# set system login announcement "welcome the switch-1101"
admin@XorPlus# commit
```

system login user

To configure a user account, use the **set system login user** command in L2/L3 configuration mode. To remove a user account, use the **delete** form of the command.

Command Syntax

set system login user *username*
delete system login user *username*

Parameter

username	The username for the new user.

Example

This example demonstrates how to create a new user account named pica8:

```
admin@Switch# set system login user pica8
```

system login user admin class

User can configure the user admin is a read-only account. The newly created user account, by default, is read-only.

Command Syntax
set system login user admin class <limit>
delete system login user admin class
Parameter
<*limit*> Configure the permission as read-only or super-user. Required select include:

- **read-only** permissions[view]
- **super-user** permission[all]
- Default value: read-only

Example
• This example demonstrates how to configure the user admin as super-user:

```
admin@XorPlus# set system login user admin class super-user
admin@XorPlus# commit
```

set system login user authentication plain-text-password

To create the password for a user account, use the **set system login user authentication plain-text-password** command in L2/L3 configuration mode. To remove the password for a user, use the delete form of the command.

NOTE: The encryption algorithm used to save user password to local is **MD5**.

Command Syntax

set system login user <*username*> **authentication plain-text-password** <*password*>
delete system login user <*username*> **authentication plain-text-password**

Parameters

Parameter	Description
user <*username*>	Name of user. The value is a string.
plain-text-password <*password*>	User's password. The value is a string that must be at least 6 characters. The password can support the below complexity: 1. Lowercase letters a-z. 2. Uppercase letters A-Z. 3. Numerics (0, 1, 2, etc.) 4. Special Characters (@, %, !, etc.)

Example

- The following example sets the password for user **alpha**; if the username does not already exist, the command will also create it.

```
admin@Switch# set system login user alpha authentication plain-text-password mypica8
 admin@XorPlus# commit
```

- This example demonstrates how to create a password for the user **admin**:

```
admin@XorPlus# set system login user admin authentication plain-text-password pica8pica8
admin@XorPlus# commit
```

system login user class

To set permissions for a user, use the **system login user class** command in L2/L3 configuration mode. By default, a newly created user account is **read-only**. To delete a user, use the **delete** form of the command.

Command Syntax

set system login user *username* **class** [**read-only** | **super-user**]
delete system login user *username* **class**

Parameters

username	The name of the user.
read-only	(Optional) This keyword gives view-only or read-only permissions to user. This is the default option.
super-user	(Optional) This keyword gives all permissions to user. The default option is **read-only**.

Example

The following example configures a **super-user** account named alpha:

```
admin@Switch# set system login user alpha class super-user
```

set system timezone

User can configure local time zone or delete it.

Command Syntax
set system timezone <*time-zone*>
delete system timezone

Parameter
•<*time-zone*>The effective value is a time zone.

Example
• This example demonstrates how to set local time zone to Shanghai:

```
admin@XorPlus# set system timezone Asia/Shanghai
admin@XorPlus# commit
```

set system ntp server-ip

The **set system ntp server-ip** command configures the IP address of the remote NTP server.

Note: the route between NTP server and NTP source interface is required to be reachable.

Command Syntax

set system ntp server-ip <*ipv4-address*>

Parameter

Parameter	Description
server-ip <*ipv4-address*>	Specifies the IPv4 address of the remote server. The value is an IPv4 address, e.g. 192.168.10.100.

Example

- Configure the IP address of the remote NTP server.

```
admin@XorPlus# set system ntp server-ip 192.168.10.100
admin@XorPlus# commit
```

set system ntp source-interface

The **set system ntp source-interface** command configures the local source interface that sends NTP packets.

Command Syntax

set system ntp source-interface <*source-interface*>

Parameter

Parameter	Description
source-interface <*vlan-interface*>	Specifies the NTP source interface. The value could be **eth0**, L3 VLAN interface, loopback interface, routed interface or sub-interface. Indicates the local interface that sends the NTP packets.

Usage Guidelines

Configure the local source interface for sending/receiving NTP packets, so that the IP address of another interface on the device cannot be used as the destination address of a reply packet, which is convenient for a user to subsequently deploy a flow control policy.

Notes:

- If the NTP source interface is configured, the source interface will be used for the NTP connection.
- If the user defined VRF is configured, and NTP is enabled (in default VRF or management VRF) without configuring the NTP source interface, the system will continuously print an error syslog like the following.

> *Apr 13 2021 15:05:47 Xorplus daemon.info : failed to init interface for address 22.1.1.201*
>
> *Apr 13 2021 15:10:47 Xorplus daemon.err : bind(41) AF_INET 21.1.1.201#123 flags 0x19 failed: Cannot assign requested address*

Example

- Configure the local source interface that sends NTP packets.

```
admin@Xorplus# set system ntp source-interface vlan100
admin@Xorplus# commit
```

set system ntp vrf mgmt-vrf

The **set system ntp vrf mgmt-vrf** command configures to run the NTP protocol inmanagement VRF.

Command Syntax

set system ntp vrf mgmt-vrf

Parameter

None.

Usage Guidelines

NTP protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding NTP server is required to be route reachable in the VRF running NTP protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the NTP protocol to run in the management VRF.

```
admin@Xorplus# set system syslog vrf mgmt-vrf
admin@Xorplus# commit
```

set interface gigabit-ethernet ptp mode

The **set interface gigabit-ethernet ptp mode** command configures the device interface as the E2ETC node type, and enables the PTP function on the interface.

Command Syntax

set interface gigabit-ethernet <*port*> **ptp mode** {e2etransparent | none}

Parameter

Parameter	Description
port	Ethernet switching port identifier, the valid ports range: 1-52.
ptp mode {e2etransparent | none}	Configure the PTP mode on a switch interface: • e2etransparent: configures the device interface as the E2ETC node type and enables the PTP function on the interface. • none: disable the PTP function on the interface.

Note: the PTP function can only be configured on the physical interface.

Example

• Configure the port te-1/1/25 that receiving PTP messages and the port te-1/1/26 that sends PTP packets as E2ETC node.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/25 ptp mode e2etransparent
admin@Xorplus# set interface gigabit-ethernet te-1/1/26 ptp mode e2etransparent
```

set system services ssh connection-limit

The **set system services ssh connection-limit** command configures the SSH connection limit per source IP address.

Command Syntax
set system services ssh connection-limit <*int*>
delete system services ssh connection-limit

Parameter
• <*int*> It is the maximum number of allowed connections,the valid number range 0-250. Default value is 0, which removes the connection limit.

Example
• This example demonstrates how to configure the SSH maximum number of connections as 5:

```
admin@XorPlus# set system services ssh connection-limit 5
admin@XorPlus# commit
```

set system services ssh disable

The set system services ssh disable command configures the permission of the SSH login.

Command Syntax
set system services ssh disable <*bool*>
delete system services ssh disable

Parameter
•<*bool*> The effective value is **true** or **false**. If the value is true, SSH login is disabled. If value is false, SSH login is enabled.

Example
• This example demonstrates how to configure SSH login as permission:

```
admin@XorPlus# set system services ssh disable false
admin@XorPlus# commit
```

set system services ssh protocol-version v2

This command refers to which specific ssh protocol version is supported. User can configure it or delete it.

Command Syntax
set system services ssh protocol-version v2
delete system services ssh protocol-version

Example
• This example demonstrates how to set the specific ssh protocol versions supported to v2:

```
admin@XorPlus# set system services ssh protocol-version v2
admin@XorPlus# commit
```

set system services ssh rate-limit

User can configure the maximum number of connections per minute and per source IP address or delete the configuration.

Command Syntax
set system services ssh rate-limit <*int*>
delete system services ssh rate-limit

Parameter
•<*int*> The effective value type is int. The valid number range 1-20.

Example
• This example demonstrates how to set the maximum number of connections per minute to 2:

```
admin@XorPlus# set system services ssh rate-limit 2
admin@XorPlus# commit
```

set system services ssh root-login

User can configure allow or deny root access via ssh or delete the limits of authority.

Command Syntax
set system services ssh root-login <*limit*>
delete system services ssh root-login

Parameter
• <*limit*> Configure allow or deny root access via ssh. Required select include:

- **allow** allow root access via ssh
- **deny** do not allow root access via ssh

Example
• This example demonstrates how to allow the root access via ssh:

```
admin@XorPlus# set system services ssh root-login allow
admin@XorPlus# commit
```

set system services ssh idle-timeout

The **set system services ssh idle-timeout** command configures the idle timeout for SSH connections.

Command Syntax

set system services ssh idle-timeout <*timeout-value*>

Parameter

Parameter	Description
idle-timeout <*timeout-value*>	Specifies the idle timeout for SSH connections. The value is an integer, in seconds, that ranges from 0 to 2000000. The default value is 0, which means no idle timeout for SSH user.

Usage Guidelines

If the SSH user logs in to the system but doesn't perform any for a long time, the SSH channel resources would be occupied for a long time thus making it difficult or impossible for other users to log in to the system. The SSH idle timeout duration is configured to release SSH resources in time. The SSH connection will be automatically disconnected if the SSH user who logged in to the system doesn't perform any operation within the SSH idle timeout duration. The following disconnect prompt is printed:

Connection to 10.10.51.193 closed by remote host.

Connection to 10.10.51.193 closed.

NOTE:

- The idle timeout timer is restarted each time the SSH user perform an operation.
- The configuration takes effect only on the next SSH login.
- The same idle timeout value is available for all the SSH users.

Example

- Configure the idle timeout for SSH user to 60s.

```
admin@Xorplus# set system services ssh idle-timeout 60
```

set system services ssh port

The **set system services ssh port** command changes the listening port number of the SSH server.

Command Syntax

set system services ssh port <*port-number*>

Parameter

Parameter	Description
port <*port-number*>	Specifies the listening port number of the SSH server. The value is an integer ranging from 1 to 65535. The default listening port number of the SSH server is 22.

Usage Guidelines

Users can use this command to configure the new port number of SSH server to prevent attackers from accessing the standard port of SSH service and ensure security.

Note that,

If the modified port number is not 22, the client needs to specify port number when logging in using SSH.

Example

- Change the listening port number of the SSH server to 30.

```
admin@Xorplus# set system services ssh port 30
admin@Xorplus# commit
```

set system snmp-acl security-name network

The **set system snmp-acl security-name network** command configures SNMP access control white list.

Command Syntax

set system snmp-acl [**security-name** <*community-name*>] **network** <*ip/mask*>

Parameter

Parameter	Description
security-name <*community-name*>	Optional. Specifies the name of a community. The value is a string. It is a **community name** for SNMPv1/SNMPv2, **security name** for SNMPv3.
network <*ip/mask*>	Specifies the network where the SNMP queries come from. The format is *IPv4/mask or IPv6/mask*. For example, 10.10.10.0/24.

Usage Guidelines

SNMP ACL has two types of access control white list: As-per User List and Global List.

- As-per User List

The SNMP ACL that specifies a security name can be configured with multiple networks and is called the as-per user list. For example,

```
admin@XorPlus# set system snmp-acl security-name public network 10.10.50.0/24
```

Where "security-name" is the **community name** for SNMPv1 and SNMPv2, and the **security name** for SNMPv3.

- Global List

SNMP ACLs that do not specify a security name but only networks are called the global list. For example,

```
admin@XorPlus# set system snmp-acl network 10.10.50.0/24
admin@XorPlus# set system snmp-acl network 10.10.51.0/24
```

The global list is applied to NMS that are not configured with an as-per user list.

NOTE:

- Multiple as-per user lists of different networks can be configured under one security name.
- If an SNMP ACL with security name is configured, but no network list is configured under this security name, this as-per user list is empty and invalid, then global list matching will be performed.

Example

- Configure an SNMP ACL as-per user list, NMS with the security name **public** and from network 10.10.50.0/24 can access the device.

```
admin@XorPlus# set system snmp-acl security-name public network 10.10.50.0/24
admin@XorPlus# commit
```

- Configure an SNMP ACL global list, NMS from 192.168.10.0/24 can access the device.

```
admin@XorPlus# set system snmp-acl network 192.168.10.0/24
admin@XorPlus# commit
```

set system syslog server-ip

The **set system syslog server-ip** command configures the remote syslog server on the switch, including IP address, port number, transmission protocol and source interface. After user configures the syslog server IP address, the log files will be sent to the syslog server.

The **delete system syslog server-ip** command deletes the configuration of remote syslog server.

Command Syntax
set system syslog server-ip <*ip_address*> [**port** <*port_number*> | **protocol** <**tcp | udp**> | **source-interface** <*source-interface*>]

Parameter

Parameter	Description
server-ip <*ip_address*>	Specifies IP address of a remote syslog server. It could be an IPv4 address or IPv6 address.
port <*port_number*>	Optional. Specifies the port of the remote syslog server. The value is an integer type.
protocol <**tcp	udp**>	Optional. Specifies the transmission protocol for the remote syslog server. The value could be **tcp** or **udp**.
source-interface <*source-interface*>	Optional. Specifies the source interface for sending/receiving syslog messages, e.g. vlan20, eth0, routed interface, sub-interface or loopback.

Notes:

- The IP address of the source interface will be used as the source IP in the IP header after syslog message is routed.
- If syslog uses **TCP** protocol, source-interface can't be configured at the same time.

Example
• This example configures how to set the IP address of the remote syslog server.

```
admin@XorPlus# set system syslog server-ip 192.168.1.1
admin@XorPlus# commit
```

set system syslog local-file

The **set system syslog local-file** command sets the local save location of the syslog file.

Command Syntax

set system syslog local-file <*location*>

Parameter

Parameter	Description
local-file <*location*>	Specifies the local save location of the syslog. The value could be **disk** or **ram**. • **disk**: saves the syslog to disk, the path is /var/log. • **ram**: saves the syslog to RAM, the path is /tmp/log. By default, the syslog is kept in RAM.

Usage Guidelines

By default, the syslog file stays in RAM. When the system is powered off and restarted, the syslog file in RAM will be cleared. You can configure the syslog to be saved to disk. When the system is powered off and restarted, the syslog saved to disk will still exist.

Example

- Set the local save location of the syslog file to disk.

```
admin@XorPlus# set system syslog local-file disk
admin@XorPlus# commit
```

set system syslog vrf mgmt-vrf

The **set system syslog vrf mgmt-vrf** command configures to run the syslog service in management VRF.

Command Syntax

set system syslog vrf mgmt-vrf

Parameter

None.

Usage Guidelines

Syslog service runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding syslog server is required to be route reachable in the VRF running syslog service.

Note: The latest configuration overrides the previous one.

Example

- Configure the syslog service to run in the management VRF.

```
admin@Xorplus# set system syslog vrf mgmt-vrf
admin@Xorplus# commit
```

set system usb disable

The **set system usb disable** command configures whether to disable all external USB interfaces of the switch.

Command Syntax

set system usb disable [**true | false**]

Parameter

Parameter	Description
disable [**true	false**]	Configures whether to disable the USB interfaces. The value is **true** or **false**. **true**: disables the USB interface. **false**: enables the USB interface. The default value is **false**.

Example

- Disable the USB interfaces.

```
admin@Xorplus# set system usb disable true
admin@Xorplus# commit
```

- Enable the USB interfaces.

```
admin@Xorplus# set system usb disable false
admin@Xorplus# commit
```

set system management-ethernet eth0 ip-address {IPv4 | IPv6}

The **set system management-ethernet eth0 ip-address** {**IPv4** | **IPv6**} command sets a static IP address for management interface eth0.

Command Syntax

set system management-ethernet eth0 ip-address {**IPv4** | **IPv6}** <*ip_address*>

Parameter

Parameter	Description
{**IPv4** | **IPv6}** <*ip_address*>	Specifies the IP address for management interface eth0. When assigning an IPv4 address, the value is in dotted decimal notation. When assigning an IPv6 address, the value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers.

Example

- Set the IP address 192.168.10.5/24 for management interface eth0.

```
admin@Xorplus# set system management-ethernet eth0 ip-address IPv4 192.168.10.5/24
admin@Xorplus# commit
```

set system management-ethernet eth0 ip-gateway {IPv4 | IPv6}

The **set system management-ethernet eth0 ip-gateway** {**IPv4** | **IPv6**} command sets the gateway address for management interface eth0.

Command Syntax

set system management-ethernet eth0 ip-gateway {**IPv4** | **IPv6}** <*ip_address*>

Parameter

Parameter	Description
{**IPv4** | **IPv6}** <*ip_address*>	Specifies the gateway address for management interface eth0. For IPv4 address, the value is in dotted decimal notation. For IPv6 address, the value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers.

Example

- Set the gateway address 192.168.10.1 for management interface eth0.

```
admin@Xorplus# set system management-ethernet eth0 ip-gateway IPv4 192.168.10.1
admin@Xorplus# commit
```

show system management-ethernet

The **show system management-ethernet** command shows the configuration information, status and traffic statistics information of the management interface.

Command Syntax

show system management-ethernet

Parameter

None.

Example

- Run **run show system management-ethernet** command to view the configuration information, status and traffic statistics information of the management interface.

```
admin@Xorplus# run show system management-ethernet
eth0    Hwaddr: 68:21:5f:7f:10:c5       State: UP
        Gateway  : 192.168.10.1
        Inet addr:
                  192.168.10.5/24
                  fe80::6a21:5fff:fe7f:10c5/64
    Traffic statistics
        Input Packets.....................222156
        Input Bytes.......................13775674
        Output Packets.....................1471
        Output Bytes......................140558

eth1    Hwaddr: 68:21:5f:7f:10:c9       State: UP
        Inet addr:
                  fe80::6a21:5fff:fe7f:10c9/64
    Traffic statistics
        Input Packets.....................0
        Input Bytes.......................0
        Output Packets.....................63
        Output Bytes......................4546
```

run request system reboot

The **run request system reboot** command restarts the device.

Command Syntax

run request system reboot *<description>*

Parameters

Parameter	Description
<description>	Optional. Add a description in the syslog before the system reboots by using **run request system reboot** command. The value is a string. If the description contains spaces, we need to enclose the whole string in double quotes.

Usage Guidelines

The command enables you to restart the device remotely.

After executing the reboot command, PICOS will automatically save the user configuration and restart the device with system diagnostics.

As system reboot will cause service interruption, so be cautious to use this command.

By configuring the description parameter, the system prints a system log with this description information before the system reboots.

- The log message containing this description is in the syslog file */var/log/messages*.
- The log message containing this description information is at the info level. To display the log message, you need to set the log-level to info or trace. Otherwise, the system will not record this log.
- The log message containing this description information is recorded only in the scenarios when the system is restarted by using run request system reboot *<description>* command. But in the scenarios of restarting the system when manually powered off or device fault, the system will not record the log message containing this description information.

Example

- Reboot PICOS.

```
admin@Xorplus# run request system reboot
```

- Reboot PICOS with the description information “Hello World”.

```
admin@Xorplus# set system syslog local-file disk   // Set the system log file to save to disk.
admin@Xorplus# run request system reboot "Hello World"
admin@Xorplus:~$ tail -f /var/log/messages       // Check the system logs.
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]Redundant power supply unit(RPSU) 1 plug in.
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]Redundant power supply unit(RPSU) 1 power on
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]rpsu 2 status changed from PSU_STATUS_INVALID to PSU_STATUS_PL
Jan  3 1970 01:08:59 Xorplus local0.warning : [LOGIN]Redundant power supply unit(RPSU) 2 plug in.
Jan  3 1970 01:09:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:10:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:11:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:11:59 Xorplus auth.info : Accepted password for admin from 10.10.50.143 port 58420 ssh2
Jan  3 1970 01:12:10 Xorplus auth.info : Accepted password for admin from 10.10.50.143 port 58422 ssh2
Jan  3 1970 01:12:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:13:54 Xorplus local0.debug : [LOGIN]Run auto switch fan controller
Jan  3 1970 01:14:21 Xorplus local0.info : [LOGIN]Hello World  //The user configured reboot description log.

Broadcast message from root@Xorplus (Sat Jan  3 01:14:21 1970):


The system is going down for reboot NOW!


Broadcast message from root@Xorplus (Sat Jan  3 01:14:22 1970):
```

```
The system is going down for reboot NOW!
Jan  3 1970 01:14:22 Xorplus user.notice : shutting down for system reboot
[ ok  [....] Stopping internet superserver: inetd.
[ ok ] Stopping: L2/L3.............
[ ok ] Asking all remaining processes to terminate...done.
[ ok ] All processes ended within 1 seconds...done.
[ ok ] Stopping enhanced syslogd: rsyslogd.
[....] Deconfiguring network interfaces...Internet Systems Consortium DHCP Client 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
```

run show system hwinfo

The **run show system hwinfo** command displays the hardware information of PICOS switch.

Command Syntax

run show system hwinfo

Parameter

None.

Exampe

- Display the hardware information of PICOS switch.

```
admin@Xorplus# run show system hwinfo
Product Name: N3208PX-ON
Part Number: 0JDFTF
Serial Number: CN0JDFTFDND0083M0100
Base MAC Address: 20:04:0F:01:63:47
Manufacture Date: 02/22/2020 14:50:07
Device Version: 1
Label Revision: A00
Platform Name: armv7a-dellemc_n3208px_iproc-r0
Loader Version: 4.39.1.0-4
MAC Addresses: 128
Manufacturer: DND00
Country Code: CN
Vendor Name: Dell EMC
Diag Version: 4.39.3.0-1
Service Tag: 8VMGXC2
Vendor Extension: 0x00 0x00 0x02 0xA2
CRC-32: 0x4260903C(Valid)


admin@Xorplus# run show system hwinfo service-tag
Service Tag: 8VMGXC2
```

ping

The **ping** command is a method for troubleshooting the accessibility of devices and outputs the statistics results.

NOTE:

When ping a link-local address, the outband VLAN interface must be specified together, otherwise it will result link unreachable.

Command Syntax

- From the "**>**" prompt, use the following format,

ping <*ip-address*> [**interface** <*interface-name*>] [**packets** <*packets*>] [**vrf** <**mgmt-vrf** | *vrf-name*>] [**source** <*source-ip-address*>] [**deadline** <*deadline-time*>] [**ttl** <*ttl-value*>] [**interval** <*interval-value*>] [**pattern** <*pattern-value*>] [**size** <*size-value*>] [**tos** <*tos-value*>]

- From the "**#**" prompt, add **run** in front of the command,

run ping <*ip-address*> [**interface** <*interface-name*>] [**packets** <*packets*>] [**vrf** <**mgmt-vrf** | *vrf-name*>] [**source** <*source-ip-address*>] [**deadline** <*deadline-time*>] [**ttl** <*ttl-value*>] [**interval** <*interval-value*>] [**pattern** <*pattern-value*>] [**size** <*size-value*>] [**tos** <*tos-value*>]

Parameter

Parameter	Description
<*ip-address*>	Specifies the domain name or IPv4/IPv6 address of the destination host.
interface <*interface-name*>	Optional. Specifies the outgoing interface which can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
packets<*packets*>	Optional. Specifies the number of ICMP Echo Request packets sent.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be mgmt-vrf or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.
source <*source-ip-address*>	Optional. Specifies the source IP address of the ICMP Echo Request message. If the source IP address is not specified, the IP address of the outbound interface is used as the source IP address of the ICMP Echo Request message.
deadline <*deadline-time*>	Optional. Specify a timeout, in seconds, before ping exits regardless of how many packets have been sent or received. In this case ping does not stop after count packet are sent, it waits either for deadline to expire or until count probes are answered or for some error notification from network.
ttl <*ttl-value*>	Optional. Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 device that the message reaches sends an ICMP timeout message to the source host, indicating that the destination host is unreachable. The value is an integer that ranges from 1 to 255.
interval <*interval-value*>	Optional. Specify the interval for sending ICMP Echo Request message. The value is an integer in second.
pattern <*pattern-value*>	Optional. Specifies pad characters for ICMP Echo Request messages. By configuring pad characters for ICMP Echo Request messages, you can identify a specific message among the large number of received ICMP Echo Reply messages. The value is a hexadecimal integer.
size <*size-value*>	Optional. Specifies the maximum payload length of an ICMP Echo Request message. The value is an integer.
tos <*tos-value*>	Optional. Specifies the ToS value of the sent ICMP Echo Request messages. The ToS value is used to set the packet priority. The value is an integer that ranges from 0 to 254.

Example

- Check whether the host at 10.10.51.1 is reachable.

```
admin@Xorplus> ping 10.10.51.1
PING 10.10.51.1 (10.10.51.1) 56(84) bytes of data.
64 bytes from 10.10.51.1: icmp_seq=1 ttl=64 time=1.94 ms
```

```
64 bytes from 10.10.51.1: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 10.10.51.1: icmp_seq=3 ttl=64 time=2.00 ms
64 bytes from 10.10.51.1: icmp_seq=4 ttl=64 time=146 ms
64 bytes from 10.10.51.1: icmp_seq=5 ttl=64 time=2.01 ms


--- 10.10.51.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.943/30.832/146.173/57.670 ms
```

traceroute

The **traceroute** command is used to check the route of packets when travelling from the source to the destination. When the network fails, the user can use this command to troubleshooting the fault point.

Command Syntax

- From the "**>**" prompt, use the following format,

traceroute <*ip-address*> [**vrf** <**mgmt-vrf** | *vrf-name*>]

- From the "**#**" prompt, add **run** in front of the command,

run traceroute <*ip-address*> [**vrf** <**mgmt-vrf** | *vrf-name*>]

Parameter

Parameter	Description
<*ip-address*>	Specifies the domain name or IPv4/IPv6 address of the destination host.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be **mgmt-vrf** or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Example

- Traceroute the gateways for the host with the IP address 10.10.50.11.

```
admin@Xorplus> traceroute 10.10.50.11
traceroute to 10.10.50.11 (10.10.50.11), 30 hops max, 60 byte packets
 1  bogon (10.10.51.1)  3.063 ms  3.214 ms  3.370 ms
 2  bogon (10.10.50.11)  0.195 ms  0.172 ms  0.201 ms
```

- Traceroute the gateways for the host with the IP address fc00::3.

```
admin@Xorplus> traceroute fc00::3
traceroute to fc00::3 (fc00::3), 30 hops max, 60 byte packets
 1  bogon (FC00:1::3)  15 ms  20 ms  30 ms
 2  bogon (FC00::3)  1901 ms  1207 ms  3020 ms
```

tftp

The **tftp** command is used to transfer files between the local device and the TFTP server by TFTP protocol.

Command Syntax

- **Download a file:**
  - From the ">" prompt, use the following format,

    file tftp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
  - From the "#" prompt, add **run** in front of the command,

    run file tftp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
- **Upload a file:**
  - From the ">" prompt, use the following format,

    file tftp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
  - From the "#" prompt, add **run** in front of the command,

    run file tftp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]

Parameter

Parameter	Description
get	Download a file.
put	Upload a file.
remote-file <*remote-file-path*>	Specifies the file path on TFTP server. The value is a string.
local-file <*local-file-path*>	Specifies the file path on local device. The value is a string.
ip-address <*ip-address*>	Specifies the IPv4/IPv6 address or host name for the TFTP server. The value is a string.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be **mgmt-vrf** or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Usage Guidelines

Use the TFTP service to upload or download files with the following precautions:

- Usually, the TFTP server specifies a directory as the **default TFTP directory**, when use the **tftp get remote-file** <*remote-file-path*> command, don't need give the full path for the file, just type the sub-directory of the default directory.

  For example, suppose there is a file **fileA** in the default TFTP directory, we can run the following command to download this file:

```
Admin@Xorplus# run file tftp get remote-file fileA
```

- On the PICA8 switch, the TFTP downloaded file is saved in directory **/cftmp/** by default.

Example

- Download file syslog.txt from the root directory of the TFTP server to the local device. The IP address of the TFTP server is 10.1.1.1. Save the downloaded file to the local device as file syslog.bak.

```
admin@Xorplus> file tftp get remote-file syslog.txt local-file syslog.bak ip-address 10.1.1.1
```

set protocols sflow collector vrf mgmt-vrf

The **set protocols sflow collector vrf mgmt-vrf** command configures to run the sFlow service in management VRF.

Command Syntax

set protocols sflow collector <*ip-address*> **vrf mgmt-vrf**

Parameter

Parameter	Description
collector <*ip-address*>	Specifies an IP address of the sFlow collector. The value is an IPv4/IPv6 address.

Usage Guidelines

SFlow service runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding collector is required to be route reachable in the VRF running sFlow service.

Note: The latest configuration overrides the previous one.

Example

- Configure the sFlow service to run in the management VRF.

```
admin@Xorplus# set protocols sflow collector 10.10.10.1 vrf mgmt-vrf
admin@Xorplus# commit
```

scp

The **scp** command is used to transfer files between the local device and the SCP server.

Command Syntax

- **Download a file:**
  - From the ">" prompt, use the following format,

    file scp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
  - From the "#" prompt, add **run** in front of the command,

    run file scp get remote-file <*remote-file-path*> [**local-file** *local-file-path*] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
- **Upload a file:**
  - From the ">" prompt, use the following format,

    file scp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]
  - From the "#" prompt, add **run** in front of the command,

    run file scp put local-file <*local-file-path*> [**remote-file** <*remote-file-path*>] **ip-address** <*ip-address*>[**vrf** <**mgmt-vrf** | vrf-name>]

Parameter

Parameter	Description
get	Download a file.
put	Upload a file.
remote-file <*remote-file-path*>	Specifies the file path on SCP server. The value is a string.
local-file <*local-file-path*>	Optional. Specifies the file path on local device. The value is a string.
ip-address <*ip-address*>:<*port*>	Specifies the IPv4/IPv6 address and port for the SCP server. The value is a string.
vrf <**mgmt-vrf** | *vrf-name*>	Optional. Specifies a VRF name. The value is a string that could be **mgmt-vrf** or a user-defined VRF name. • **mgmt-vrf**: management VRF is specified. • *vrf-name:* a user-defined VRF set by using command **set ip vrf** <*vrf-name*> [**description** <*string*>]. **NOTE:** • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Usage Guidelines

Use the SCP service to upload or download files with the following precautions:

- Usually, the SCP server specifies a directory as the **default SCP directory**, when using the **scp get remote-file** <*remote-file-path*> command, don't need give the full path for the file, just type the subdirectory of the default directory.

  For example, suppose there is a file **fileA** in the default SCP directory, we can run the following command to download this file:

```
admin@Xorplus> file scp get remote-file fileA
```

- On the Pica8 switch, the SCP downloaded file is saved in directory **/cftmp/** by default.

Example

- Download file syslog.txt from the root directory of the SCP server to the local device. The IP address of the SCP server is 10.1.1.1. Save the downloaded file to the local device as file syslog.bak.

```
admin@Xorplus> file scp get remote-file syslog.txt local-file syslog.bak ip-address 10.1.1.1
```

set system login banner

The **set system login banner** command configures the header information displayed on a terminal before login.

Command Syntax

set system login banner <*text*>

Parameter

Parameter	Description
banner <*text*>	Specifies the banner content. The value is a string. Configure the banner information you want to print in double quotes.

Example

- Configure a login banner before login.

```
admin@Xorplus# set system login banner "Welcome to system!"
```

upgrade2 image-file

The **upgrade2 image-file** command upgrades the system by using upgrade2 command from the CLI operational mode or configuration mode.

Command Syntax

upgrade2 image-file <*image-name*>

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

The default directory for image file is */cftmp* if users do not specify the file path.

Example

- Upgrade the system by using upgrade2 command.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin
```

upgrade2 image-file backup-file

The **upgrade2 image-file backup-file** command upgrades the system by using upgrade2 command from the CLI operational mode or configuration mode and saves the user files during the upgrade process.

Command Syntax

upgrade2 image-file <*image-name*> **backup-file** <*backup-file*>

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).
backup-file <*backup-file*>	Specify a user defined backup list (*.lst).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

During the upgrade process, the switch can automatically back up the following files in the following directories from the previous PICOS system:

```
/etc/passwd
/etc/shadow
/etc/group
/etc/gshadow
/etc/resolv.conf
./etc/network/interfaces
/etc/picos/picos_start.conf
/etc/picos/switch-public.key
/etc/picos/pica.lic
/pica/config/pica_startup.boot
/pica/config/pica.conf.01
/pica/config/pica.conf.02
/pica/config/pica.conf.03
/pica/config/pica.conf.04
/pica/config/pica.conf.05
/ovs/ovs-vswitchd.conf.db
/ovs/function.conf.db
/ovs/config/meters
/ovs/config/groups
/ovs/config/flows
/ovs/var/lib/openvswitch/pki/
/var/log/report_diag.log
/var/log/report_diag.log.1
/var/log/report_diag.log.2
/var/log/report_diag.log.3
/var/log/report_diag.log.4
/var/log/report_diag.log.5
/cftmp/upgrade.log
/cftmp/upgrade2.log
/cftmp/auto/
```

If you want to save user files that are not in the above default backup file list, you need to first create or specify a **.lst** file and then add all those files that need to be backed up to this **.lst** file. You can use the **backup-file=(*.lst)** option to achieve this, where (*.lst) is the user created file with **.lst** format or specify the file path to this

file.

The default directories for image file and backup file are */cftmp* if users do not specify the file path.

For example:

```
admin@XorPlus> sudo upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin backup-file /admin/back_files.ls
```

In this example, **back_files.lst** is a user created file. The user has already added the file to back_files.lst that needs to be saved in the event of power off.

Example

- Upgrade the system by using upgrade2 command and save the user files during the upgrade process.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin backup-file /admin/back_files.lst
```

upgrade2 image-file factory-default

The **upgrade2 image-file factory-default** command upgrades the system by using upgrade2 command and recoveries configuration to factory default settings.

Command Syntax

upgrade2 image-file <*image-name*> **factory-default**

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

Example

- Upgrade the system by using upgrade2 command and recovery configuration to factory default settings.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin factory-default
```

upgrade2 image-file use-prev-config

The **upgrade2 image-file use-prev-config** command upgrades the system by using upgrade2 command, skip the un-compatible configuration and continue loading the remaining configuration after system starts up from the reboot.

Command Syntax

upgrade2 image-file <*image-name*> **use-prev-config**

Parameter

Parameter	Description
image-file <*image-name*>	Specifies the image name with bin format (*.bin).

Usage Guidelines

Before upgrading, save the important data in Flash to the local PC through FTP or TFTP, and then upload it to the switch after the upgrade is completed.

The main function of **use-prev-config** option is to decide whether to load the previous configuration file after a system reboot when performing upgrade2 or rollback to another version. If there is a command line in the old version configuration file that is not supported in the new system, with **use-prev-config** option that command will be skipped and continue loading the remaining configuration.

By default, upgrade2 or rollback is performed without **use-prev-config** option.

The following table describes the usage of **use-prev-config** option when performing upgrade2 or rollback.

	upgrade2 (From old version to new version)	**rollback** (From current version to old version)
with use-prev-config	1. Load the configuration file of old version after system reboot. 2. If there is a command line in the old version configuration file that is not supported in the new system, skip it and continue loading the remaining configuration.	1. Load the configuration file of current version after system reboot. 2. If there is a command line in the current configuration file that is not supported in the old system, skip it and continue loading the remaining configuration.
without use-prev-config	1. Load the configuration file of old version after reboot. 2. If there is a command in the old version configuration file that is not supported in the new system, load default configuration file.	Load the old version configuration file after rebooting.

Example

- Upgrade the system by using upgrade2 command, skip the un-compatible configuration and continue loading the remaining configuration after system starts up from the reboot.

```
admin@Xorplus> upgrade2 image-file onie-installer-picos-3.7.3-91bb175-x86.bin use-prev-config
```

set system dns-server-ip

The **set system dns-server-ip** command configures an IP address for a DNS server.

Command Syntax

set system dns-server-ip <*dns-server-ip*>

Parameter

Parameter	Description
dns-server-ip <*dns-server-ip*>	Specifies the IP address of a DNS server. The value could be an IPv4 address or an IPv6 address.

Usage Guidelines

During dynamic domain name resolution, the device can send a query packet to the DNS server, requesting for the query result.

Example

- Configure a DNS server with the IP addresses 172.16.1.1.

```
admin@Xorplus# set system dns-server-ip 172.16.1.1
```

set system console idle-timeout

The **set system console idle-timeout** command configures the timeout duration for disconnection from a console connection.

Command Syntax

set system console idle-timeout <*idle-timeout*>

Parameter

Parameter	Description
idle-timeout <*idle-timeout*>	Specifies the timeout duration for disconnection from a console connection. The value is an integer that ranges from 0 to 2000000, in second. The default value is 0, indicating that the console connection remains alive until you close it.

Usage Guidelines

If a user logs in to the device and does not perform an operation from the console port, the user interface is occupied unnecessarily. You can run the **set system console idle-timeout** command to disconnect the user's terminal from the device after the timeout duration.

NOTE:

Configuration changes takes effect immediately after successfully commit.

Example

- Configure the timeout duration for disconnection from a console connection to 1800 seconds.

```
admin@Xorplus# set system console idle-timeout 1800
admin@Xorplus# commit
```

set system login multiline-banner message

The **set system login multiline-banner message** command configures the header information displayed on a terminal before login, this command can be used for printing multi-line informations.

Command Syntax

set system login multiline-banner <*line-number*> **message** <*text*>

Parameter

Parameter	Description
multiline-banner <*line-number*>	Specifies the line number. The value is an integer that ranges from 1 to 20.
message <*text*>	Specifies the banner content. The value is a string. Configure the banner information you want to print in double quotes.

Example

- Configure a multi-line login banner.

```
admin@Xorplus# set system login multiline-banner 1 message "********************NOTICE**********************"
admin@Xorplus# set system login multiline-banner 2 message "This is a property of Pica8."
admin@Xorplus# set system login multiline-banner 3 message "All users log-in are subject to company monitoring!"
admin@Xorplus# set system login multiline-banner 4 message "************************************************"
admin@Xorplus# commit
```

set system login multiline-announcement message

The **set system login multiline-announcement message** command configures the announcement message displayed on a terminal after users login, this command can be used for printing multi-line informations.

Command Syntax

set system login multiline-announcement <*line-number*> **message** <*text*>

Parameter

Parameter	Description
multiline-announcement <*line-number*>	Specifies the line number. The value is an integer that ranges from 1 to 20.
message <*text*>	Specifies the announcement message. The value is a string. **NOTE:** Configure the announcement message you want to print in double quotes.

Example

- Configure a multi-line login announcement message.

```
admin@XorPlus# set system login multiline-announcement 1 message "**********************************************"
admin@XorPlus# set system login multiline-announcement 2 message "Welcome to the system!"
admin@XorPlus# set system login multiline-announcement 3 message "**********************************************"
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

set system aaa radius source-interface

The **set system aaa radius source-interface** command sets the source interface the switch uses to connect to the RADIUS server.

Command Syntax

set system aaa radius source-interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the source interface. The value could be an L3 VLAN interface, loopback interface, routed interface or sub-interface that enabled inband management or eth0. By default, the source interface is eth0.

Usage Guidelines

NOTE:

- When using a L3 VLAN interface, loopback interface, routed interface or sub-interface as a source interface connecting to the RADIUS server, you have to enable inband management function by using commands **set system inband vlan-interface** <*vlan-interface*>, **set system inband loopback** <*loopback-interface*>, **set system inband routed-interface** <*routed-interface*>.
- Remember to specify an IP address for the source interface.

Example

- Set the source interface the switch uses to connect to the RADIUS server to loopback interface.

```
admin@Xorplus# set l3-interface loopback lo address 10.1.1.1 prefix-length 32
admin@Xorplus# set system aaa radius source-interface loopback
```

- Set the source interface the switch uses to connect to the RADIUS server to L3 VLAN interface.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/23 family ethernet-switching native-vlan-id 100
admin@Xorplus# set l3-interface vlan-interface vlan100 address 10.10.51.129 prefix-length 24
admin@Xorplus# set vlans vlan-id 100 l3-interface vlan100
admin@Xorplus# set system inband vlan-interface vlan100
admin@Xorplus# set system aaa radius source-interface vlan100
```

set protocols grpc enable

The **set protocols grpc enable** command e**nables** gRPC agent on the device, which supports the gNMI interface for dial-in mode of Telemetry technology.

The **delete protocols grpc enable** command disables the gRPC agent function on the device.

Command Syntax

set protocols grpc enable <**true | false**>

Parameter

Parameter	Description
enable <true | false>	Enables or disables gRPC agent function on the device**.** The value could be **true** or **false**. • **true**: Enables gRPC agent function**.** • **false**: Disables gRPC agent function. By default, gRPC agent function is disabled.

Example

- Enable gRPC agent.

```
admin@Xorplus# set protocols grpc enable true
admin@Xorplus# commit
```

set protocols grpc port

The **set protocols grpc port** command configures the listening port number for the gRPC agent.

Command Syntax

set protocols grpc port <*port-number*>

Parameter

Parameter	Description
port <*port-number*>	Specifies the listening port number for the gRPC agent. The value is an integer that ranges from 1024 to 65535. The default value is 9339.

Example

- Configure the listening port number for the gRPC agent.

```
admin@Xorplus# set protocols grpc port 10500
admin@Xorplus# commit
```

set system ztp enable

The **set system ztp enable** command can be used to enable or disable ZTP (Zero Touch Provisioning) function.

Command Syntax
set system ztp enable <true | false>

Parameter

Parameter	Description
enable <true | false>	Configures whether to enable or disable the ZTP function. The value is **true** or **false**. **true**: enables the ZTP function. **false**: disables the ZTP function. The default value is **true**.

Usage Guidelines

By default, the ZTP function is enabled, and the ZTP process is automatically performed when the device boots up with empty configuration. Users can disable ZTP function if they do not want the device to perform ZTP process when booting with empty configuration.

Example

• Disable the ZTP function.

```
admin@XorPlus# set system ztp enable false
admin@XorPlus# commit
```

telnet

The **telnet** command is used to connect to remote servers from the current device using the Telnet protocol. Before using the telnet command to connect to a Telnet server, the Telnet client and the Telnet server need to be route reachable, and the Telnet service must be enabled on the Telnet server side.

Command Syntax

- From the "**>**" prompt, use the following format,

telnet {<*ip-address*>|<*host-name*>} [<*port-number*>] [**vrf** <*vrf-name*>]

- From the "**#**" prompt, add **run** in front of the command,

run telnet {<*ip-address*>|<*host-name*>} [<*port-number*>] [**vrf** <*vrf-name*>]

Parameter

Parameter	Description
<*ip-address*>|<*host-name*>	Specifies the IPv4/IPv6 address or host name of a remote system.
<*port-number*>	Optional. Specifies the TCP port number on which the remote device provides Telnet service. The value is an integer that ranges from 1 to 65535. The default value is 23.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Example

- Establish a Telnet connection with a remote device in default VRF.

```
admin@PICOS>  telnet 10.10.51.205 vrf mgmt-vrf
Trying 10.10.51.205...
Connected to 10.10.51.205.
Escape character is '^]'.


User Access Verification

Username:
```

- Establish a Telnet connection with a remote device in management VRF.

```
admin@PICOS>  telnet 10.10.51.25 vrf mgmt-vrf
Trying 10.10.51.205...
Connected to 10.10.51.205.
Escape character is '^]'.


User Access Verification

Username:
```

set system start-shell-sh password

The **set system start-shell-sh password** command configures the password when using command ***run start shell sh*** to entering Linux shell.

The **delete system start-shell-sh password** command deletes the configuration.

Command Syntax

set system start-shell-sh password *<password>*

delete system start-shell-sh password

Parameter

Parameter	Description
password *<password>*	Specifies the password for entering Linux shell. The value is a string, spaces are not allowed, case-sensitive, and can be 6 to 48 characters long. By default, there is no password for entering Linux shell.

Usage Guidelines

The configuration takes effect immediately after successfully commit.

When showing the configuration, the password is displayed as ciphertext.

Example

- Configure the password for entering Linux shell and enter Linux shell with this password.

```
admin@PICOS# set system start-shell-sh password 123456abc
admin@PICOS# commit
admin@PICOS# run start shell sh 123456abc
admin@PICOS:~$
```

set system services telnet disable

The **set system services telnet disable** command can be used to enable or disable the telnet service function. The Pica8 switch supports functioning as a telnet server. To enable the telnet server function, users can enable the telnet service by using this command.

The **delete system services telnet disable** command deletes the configuration.

NOTEs:

- Users need to enable telnet service to enable telnet server function on the device.
- Telnet service is insecure. Do not enable a telnet server if you don't know what exactly it may mean.
- Limit to a maximum of 20 connections within 10 seconds.
- Terminate the session in 60 seconds if the connection is not successful.

Command Syntax

set system services telnet disable <**true | false**>

delete system services telnet disable

Parameter

Parameter	Description
enable <**true	false**>	Enable or disable telnet service. The value could be **true** or **false**. • **true**: Enable telnet service. • **false**: Disable telnet service. By default, telnet service is disabled.

Example

- Enable telnet service.

```
admin@PICOS# set system services telnet disable false
admin@PICOS# commit
```

Interface Configuration Commands

This section contains descriptions of the CLI commands that this chapter references.

- interface aggregate-balancing hash-mapping field ethernet-destination-address disable
- interface aggregate-balancing hash-mapping field ethernet-source-address disable
- interface aggregate-balancing hash-mapping field ethernet-type disable
- interface aggregate-balancing hash-mapping field ingress-interface disable
- interface aggregate-balancing hash-mapping field ip-destination disable
- interface aggregate-balancing hash-mapping field ip-protocol disable
- interface aggregate-balancing hash-mapping field ip-source disable
- interface aggregate-balancing hash-mapping field port-destination disable
- interface aggregate-balancing hash-mapping field port-source disable
- interface aggregate-balancing hash-mapping field vlan disable
- interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control
- interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port
- interface aggregate-ethernet <lag_name> backup-port delay
- interface aggregate-ethernet <lag_name> backup-port interface
- interface aggregate-ethernet <lag_name> backup-port mode
- interface aggregate-ethernet <lag_name> crossflow enable
- interface aggregate-ethernet <lag_name> crossflow local-control
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress
- interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode
- interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id
- interface aggregate-ethernet <lag_name> hash-mapping mode
- interface aggregate-ethernet <lag_name> mtu
- interface aggregate-ethernet <lag_name> snmp-trap
- interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan
- interface aggregate-ethernet <lag_name> storm-control <mode> pps
- interface cut-through-mode
- interface ecmp max-path
- interface ethernet-switching-options buffer queue-limit
- interface ethernet-switching-options mac-table-aging-time
- interface gigabit-ethernet <port> backup-port delay
- interface gigabit-ethernet <port> backup-port interface
- interface gigabit-ethernet <port> backup-port mode
- interface gigabit-ethernet <port> crossflow enable
- interface gigabit-ethernet <port> crossflow local-control
- interface gigabit-ethernet <port> description
- interface gigabit-ethernet <port> disable
- interface gigabit-ethernet <port> ether-options flow-control
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress
- interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode
- interface gigabit-ethernet <port> family ethernet-switching native-vlan-id
- interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged
- interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>
- interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>
- interface gigabit-ethernet <port> mac-learning <boolean>
- interface gigabit-ethernet <port> mtu
- interface gigabit-ethernet <port> power-preemphasis-level
- interface gigabit-ethernet <port> snmp-trap
- interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id>
- interface gigabit-ethernet <port> storm-control <mode> kbps
- interface gigabit-ethernet <port> storm-control <mode> pps
- interface gigabit-ethernet <port> storm-control <mode> ratio <value>
- interface gigabit-ethernet <port> wred queue <value> drop_probability
- interface gigabit-ethernet <port> wred queue <value> ecn_thresh
- interface gigabit-ethernet <port> wred queue <value> enable
- interface gigabit-ethernet <port> wred queue <value> max_thresh

- interface gigabit-ethernet <port> wred queue <value> min_thresh
- interface max-acl-rule-limit <egress/ingress>
- interface max-route-limit
- IPv6 Neighbor Discovery Protocol Command Reference
  - set l3-interface routed-interface ipv6-nd adv-interval-option
  - set l3-interface routed-interface ipv6-nd home-agent-config-flag
  - set l3-interface routed-interface ipv6-nd home-agent-lifetime
  - set l3-interface routed-interface ipv6-nd home-agent-preference
  - set l3-interface routed-interface ipv6-nd managed-config-flag
  - set l3-interface routed-interface ipv6-nd mtu
  - set l3-interface routed-interface ipv6-nd other-config-flag
  - set l3-interface routed-interface ipv6-nd prefix off-link
  - set l3-interface routed-interface ipv6-nd prefix preferred-lifetime
  - set l3-interface routed-interface ipv6-nd prefix router-address
  - set l3-interface routed-interface ipv6-nd prefix valid-lifetime
  - set l3-interface routed-interface ipv6-nd ra-fast-retrans
  - set l3-interface routed-interface ipv6-nd ra-interval
  - set l3-interface routed-interface ipv6-nd ra-lifetime
  - set l3-interface routed-interface ipv6-nd reachable-time
  - set l3-interface routed-interface ipv6-nd router-preference
  - set l3-interface routed-interface ipv6-nd suppress-ra
  - set l3-interface vlan-interface ipv6-nd adv-interval-option
  - set l3-interface vlan-interface ipv6-nd home-agent-config-flag
  - set l3-interface vlan-interface ipv6-nd home-agent-lifetime
  - set l3-interface vlan-interface ipv6-nd home-agent-preference
  - set l3-interface vlan-interface ipv6-nd managed-config-flag
  - set l3-interface vlan-interface ipv6-nd mtu
  - set l3-interface vlan-interface ipv6-nd other-config-flag
  - set l3-interface vlan-interface ipv6-nd prefix off-link
  - set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime
  - set l3-interface vlan-interface ipv6-nd prefix router-address
  - set l3-interface vlan-interface ipv6-nd prefix valid-lifetime
  - set l3-interface vlan-interface ipv6-nd ra-fast-retrans
  - set l3-interface vlan-interface ipv6-nd ra-interval
  - set l3-interface vlan-interface ipv6-nd ra-lifetime
  - set l3-interface vlan-interface ipv6-nd reachable-time
  - set l3-interface vlan-interface ipv6-nd router-preference
  - set l3-interface vlan-interface ipv6-nd suppress-ra
- L3 Interface
  - run clear l3-interface statistics
  - run show l3-interface
  - run show l3-interface loopback
  - run show l3-interface routed-interface
  - run show l3-interface vlan-interface
  - set l3-interface loopback address
  - set l3-interface loopback disable
  - set l3-interface loopback vrf
  - set l3-interface routed-interface address
  - set l3-interface routed-interface description
  - set l3-interface routed-interface dhcp
  - set l3-interface routed-interface mtu
  - set l3-interface routed-interface pmtu-discovery
  - set l3-interface routed-interface rate-limit
  - set l3-interface routed-interface vrf
  - set l3-interface vlan-interface address prefix-length
  - set l3-interface vlan-interface dhcp
  - set l3-interface vlan-interface mtu
  - set l3-interface vlan-interface pmtu-discovery
  - set l3-interface vlan-interface rate-limit
  - set l3-interface vlan-interface vrf
- Port Security Commands
  - run clear port-security dynamic address
  - run clear port-security dynamic interface
  - run clear port-security port-error
  - run clear port-security sticky address
  - run clear port-security sticky interface
  - run show port-security address
  - run show port-security brief
  - run show port-security interface
  - set interface ethernet-switching-options port-error-discard timeout
  - set interface gigabit-ethernet port-security block

    - set interface gigabit-ethernet port-security mac-address vlan
    - set interface gigabit-ethernet port-security mac-limit
    - set interface gigabit-ethernet port-security sticky
    - set interface gigabit-ethernet port-security violation
- Routed Interface
    - run show interface routed-interface brief
    - run show vlans routed-vlan
    - set interface aggregate-ethernet routed-interface enable
    - set interface aggregate-ethernet routed-interface name
    - set interface aggregate-ethernet routed-interface sub-interface vlan-id
    - set interface gigabit-ethernet routed-interface enable
    - set interface gigabit-ethernet routed-interface name
    - set interface gigabit-ethernet routed-interface sub-interface
    - set vlans reserved-vlan
- run show interface diagnostics tdr
- run show interface port-index-mapping
- set interface aggregate-ethernet
- set interface aggregate-ethernet aggregated-ether-options lacp
- set interface aggregate-ethernet aggregated-ether-options lacp fallback enable
- set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout
- set interface aggregate-ethernet description
- set interface aggregate-ethernet disable
- set interface aggregate-ethernet family ethernet-switching port-mode
- set interface aggregate-ethernet family ethernet-switching vlan members
- set interface bpdu-tunneling destination-mac
- set interface ecmp hash-mapping dlb-normal
- set interface ecmp hash-mapping field ingress-interface disable
- set interface ecmp hash-mapping field ip-destination disable
- set interface ecmp hash-mapping field ip-protocol disable
- set interface ecmp hash-mapping field ip-source disable
- set interface ecmp hash-mapping field port-destination disable
- set interface ecmp hash-mapping field port-source disable
- set interface ecmp hash-mapping field vlan disable
- set interface ecmp hash-mapping randomized-load-balancing
- set interface ecmp hash-mapping round-robin-load-balancing
- set interface ecmp hash-mapping symmetric
- set interface gigabit-ethernet auto-speeds
- set interface gigabit-ethernet breakout
- set interface gigabit-ethernet cdr
- set interface gigabit-ethernet duplex auto
- set interface gigabit-ethernet ether-options 802.3ad
- set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol
- set interface gigabit-ethernet family ethernet-switching port-mode
- set interface gigabit-ethernet family ethernet-switching vlan members
- set interface gigabit-ethernet fec
- set interface gigabit-ethernet speed
- set interface gigabit-ethernet up-mode
- set management-ethernet-speed eth0
- show interface aggregate-ethernet <lag_name>
- show interface aggregate-ethernet <lag_name> dot1q-tunneling
- show interface bpdu-tunneling
- show interface brief
- show interface detail
- show interface diagnostics optics all
- show interface ecmp max-path
- show interface flexlink
- show interface gigabit-ethernet <interface>
- Uplink Failure Detection Commands
    - run show interface ufd
    - set interface ufd link-to-disable
    - set interface ufd link-to-monitor

Port Security Commands

- set interface gigabit-ethernet port-security mac-address vlan
- set interface gigabit-ethernet port-security mac-limit
- set interface gigabit-ethernet port-security sticky
- set interface gigabit-ethernet port-security violation
- set interface gigabit-ethernet port-security block
- set interface ethernet-switching-options port-error-discard timeout
- run show port-security brief
- run show port-security address
- run show port-security interface
- run clear port-security port-error
- run clear port-security sticky interface
- run clear port-security sticky address
- run clear port-security dynamic interface
- run clear port-security dynamic address

set interface gigabit-ethernet port-security mac-address vlan

The **set interface gigabit-ethernet port-security mac-address vlan** command configures a static secure MAC address.

The **delete interface gigabit-ethernet port-security mac-address vlan** command removes a static secure MAC address. No clear command can be used to remove a static secure MAC address.

Command Syntax
set interface gigabit-ethernet <*interface-name*>**port-security mac-address** <*mac-addr*> **vlan**<*vlan-id*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
mac-address <*mac-addr*>	Specifies a static secure MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. Note that, the MAC address cannot be configured to a multicast MAC or the system MAC.
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

After port security is enabled, the dynamic MAC addresses learned on the secure interface will be changed to dynamic secure MAC addresses. When the secure interface goes down and up, or device reboots or restarts, dynamic secure MAC addresses are lost and need to be re-learned.

Dynamic secure MAC addresses will be aged out by the MAC aging time.

However, static secure MAC table entries are not lost in the case of interface state changing to down or the switch restarted or rebooted. The command **set interface gigabit-ethernet** <*port-name*> **port-security mac-address** <*mac-addr*> **vlan** <*vlan-id*> can be used to configure the

static secure MAC address.

NOTE:

- Static secure MAC addresses have a higher priority than dynamic secure MAC addresses.
- Once a MAC address is bound to a port, it's not allowed to bind this MAC to another port.

Example

- Configure a static secure MAC address.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 port-security mac-address 22:00:00:00:00:00 vlan 1
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security mac-limit

The **set interface gigabit-ethernet port-security mac-limit** command configures the maximum number of secure MAC addresses that can be learned on an interface.

Command Syntax
set interface gigabit-ethernet <*interface-name*> **port-security mac-limit** <*mac-limit*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
mac-limit <*mac-limit*>	Specifies the maximum number of secure MAC addresses that can be learned by an interface. The value is an integer that ranges from 1 to 1024. The default value is 1.

Usage Guidelines

The MAC limit number is used to limit the number of secure MAC of the interface, including the number of dynamic secure MAC and manually configured static secure MAC. If sticky is enabled, MAC limit includes sticky secure MAC and static secure MAC.

A secure interface can learn only one secure MAC address by default. Set the maximum number of secure MAC addresses according to the actual networking requirement.

If you are trying to configure a static secure MAC address and it exceeds the MAC limit, your configuration is rejected and an error message is displayed. If it reaches the MAC limit and a new dynamic secure MAC address is learned, a violation action is triggered. For details about violation, please see set interface gigabit-ethernet port-security violation.

NOTE:

When setting a MAC limit value for a secure interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of the secure addresses on the interface exceeds the new value, the command is rejected. In this case, you can remove the secure addresses to the number less than the new MAC limit value.

Example

- Configure the maximum number of secure MAC addresses that can be learned on an interface.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security mac-limit 10
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security sticky

The **set interface gigabit-ethernet port-security sticky** command is used to enable or disable the sticky function on an interface.

Command Syntax
set interface gigabit-ethernet <*interface-name*> **port-security sticky** <**true** | **false**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
sticky <true | false>	Enables or disables the sticky function on an interface. The value could be **true** or **false**. • **true**: enables the sticky MAC function • **false**: disables the sticky MAC function. By default, sticky function is disabled.

Usage Guidelines

When the secure port goes down and up, dynamic secure MAC addresses will be cleared by the system. You can enable the sticky function to solve this problem.

After enabled the sticky function, the dynamic secure MAC addresses learned on the port are converted to sticky secure MAC. The sticky MAC will not be aged, and the sticky MAC table entries will not be lost when the port is down and up.

NOTE:
- When the switch reboots or restarts, sticky secure MAC addresses are lost and need to be re-learned.
- Disabling the sticky function converts the sticky secure MAC addresses on the current interface to dynamic secure MAC addresses.

Example
• Enable the sticky function on interface ge-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security sticky true
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security violation

The **set interface gigabit-ethernet port-security violation** command configures a protective action for the system to perform when the number of learned MAC addresses exceeds the MAC limit.

Command Syntax
set interface gigabit-ethernet <*interface-name*> **port-security violation** <**protect | restrict | shutdown | shutdown-temp**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
violation <**protect** | **restrict** | **shutdown** | **shutdown-temp**>	Specifies the protective action. The value could be **protect**, **restrict**, **shutdown** or **shutdown-temp**. • **protect**: Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit. • **restrict**: Discards packets with new source MAC addresses and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. • **shutdown**: Shuts the interface down, sets the interface status to error-disabled and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. User can recover the port with the **run clear port-security port-error** command. • **shutdown-temp**: Shuts the interface down temporarily, sets the interface status to error-discard and generates a warning syslog message when the number of learned MAC addresses exceeds the limit. After 20 seconds (default), the interface comes up. The **set interface ethernet-switching-options port-error-discard timeout** command configures the port recovery interval when the port security violation mode is configured to **shutdown-temp**. The default value is **protect**.

Usage Guidelines

If it reaches the MAC limit and you are trying to configure a static secure MAC address, your configuration is rejected and an error message is displayed. If it reaches the MAC limit and a new dynamic secure MAC address is added, a violation action is triggered.

Example
• Configure the protective action for the system to perform when the number of learned MAC addresses exceeds the limit to **shutdown**.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security violation shutdown
admin@XorPlus# commit
```

set interface gigabit-ethernet port-security block

The **set interface gigabit-ethernet port-security block** command configures the type of packets that will be blocked in the egress direction of the secure port.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **port-security block** <**all | broadcast | multicast | uni-multi-cast | unicast**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface name. For example, te-1/1/49, ge-1/1/1.
block <**all** | **broadcast** | **multicast** | **uni-multi-cast** | **unicast**>	Specifies the packet type which will be blocked on the egress direction of the port enabled with port security. The value could be **all**, **broadcast**, **multicast**, **uni-multi-cast** or **unicast**. • **all**: Discards all the packets in egress direction of the port. • **broadcast**: Discards only the broadcast packets in egress direction of the port. • **multicast**: Discards only the multicast packets in egress direction of the port. • **uni-multi-cast**: Discards both the unknown unicast packets and multicast packets in egress direction of the port. • **unicast**: Discards only the unknown unicast packets in egress direction of the port. By default, packets will not be blocked by port security in egress direction of the port.

Example
• Configure to discard only the broadcast packets in egress direction of the port.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 port-security block broadcast
admin@XorPlus# commit
```

set interface ethernet-switching-options port-error-discard timeout

The **set interface ethernet-switching-options port-error-discard timeout** command configures the port recovery interval when the port security violation mode is **shutdown-temp**.

Command Syntax
set interface ethernet-switching-options port-error-discard timeout <*seconds*>

Parameter

Parameter	Description
timeout <*seconds*>	Specifies the port recovery interval when the port security violation mode is **shutdown-temp**. The value is an integer, in seconds, that ranges from 10 to 300. The default value is 20 seconds.

Example
• Configure the port recovery interval when the port security violation mode is shutdown-temp.

```
admin@XorPlus# set interface ethernet-switching-options port-error-discard timeout 10
admin@XorPlus#commit
```

run show port-security brief

The **run show port-security brief** command briefly displays the port security configuration and statistics information for all the secure ports.

Command Syntax

run show port-security brief

Parameter

None.

Example

- Run the command **run show port-security brief** to briefly view the port security configuration and statistics information.

```
admin@Xorplus# run show port-security brief
Secure Port    MaxMacLimit    CurrentAddr    ViolationCount    Action
-------------------------------------------------------------------------------------------------------------------
ge-1/1/22      2              0              0                 restrict
ge-1/1/23      1              0              0                 shutdown-temp
ge-1/1/34      1              0              0                 protect
```

Table 1. Description of the run show port-security brief command output

Item	Description
Secure Port	Indicates the port enabled port security.
MaxMacLimit	Indicates the maximum number of secure MAC addresses that can be learned on the interface.
CurrentAddr	Indicates the secure MAC addresses on the interface.
ViolationCount	The number of times that violation was triggered. Note that port security violations are counted only if the port security violation mode is **restrict**, **shutdown**, or **shutdown-temp**.
Action	Indicates the protective action for the system to perform when the number of learned MAC addresses exceeds the limit. The value could be **protect**, **restrict**, **shutdown** or **shutdown-temp**.

run show port-security address

The **run show port-security address** command displays the secure MAC address table entries.

Command Syntax

run show port-security [**interface gigabit-ethernet** <*interface-name*>] **address**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Optional. Specifies a secure interface name. The value is a string. • If no interface name is specified, the secure MAC address table entries of all the secure ports are displayed. • If an interface name is specified, only the secure MAC address table entries of the specific secure port are displayed.

Example

- Run **run show port-security address** command to view the secure MAC address table entries.

```
admin@XorPlus# run show port-security address
Secure Mac Address Table
-----------------------------------------------------
Vlan MAC Address Type Interface
---- ---------------- ------- ----------
1 00:00:11:11:11:11 dynamic ge-1/1/1
1 00:00:11:11:11:12 dynamic ge-1/1/1
1 00:00:23:23:23:23 static ge-1/1/1
1 00:00:23:23:23:24 static ge-1/1/1
1 00:00:23:23:23:25 static ge-1/1/1
-----------------------------------------------------
MAC age time :300s
```

- Run **run show port-security interface gigabit-ethernet** <*interface-name*> **address** command to view the secure MAC address table entries on a secure interface.

```
admin@Xorplus# run show port-security interface gigabit-ethernet ge-1/1/34 address
            Secure Mac Address Table
-----------------------------------------------------
VLAN  MAC Address      Type     Interface
----     -----------------      -------    ----------
1       00:00:11:11:11:11  dynamic   ge-1/1/1
-----------------------------------------------------
MAC age time    :300s
```

run show port-security interface

The **run show port-security interface** command displays the detailed port security configuration and statistical information based on secure ports.

Command Syntax

run show port-securityinterface [**gigabit-ethernet** <*interface-name*>]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Optional. Specifies a secure interface name. The value is a string. • If no interface name is specified, the detailed port security configuration and statistical information of all the secure ports are displayed. • If an interface name is specified, only the detailed port security configuration and statistical information of the specific secure port are displayed.

Example

- Run **run show port-security interface** command to view the detailed port security configuration and statistical information of all the secure ports.

```
admin@Xorplus# run show port-security interface
Interface ge-1/1/22
---------------------------------------
Port Security               : enabled
Violation action            : restrict
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 2
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0

Interface ge-1/1/23
---------------------------------------
Port Security               : enabled
Violation action            : shutdown-temp
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 1
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0

Interface ge-1/1/34
---------------------------------------
Port Security               : enabled
Violation action            : protect
Block type                  : N/A
Sticky                      : false
Maximum MAC limit           : 1
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0
```

- Run command **run show port-security interface gigabit-ethernet** <*interface-name*> to view the detailed port security configuration and statistical information of a specific secure port.

```
admin@Xorplus# run show port-security interface gigabit-ethernet ge-1/1/22
Interface ge-1/1/22
---------------------------------------
Port Security               : enabled
Violation action            : restrict
Block type                  : N/A
Sticky                      : true
Maximum MAC limit           : 2
Total MAC addresses         : 0
Configured MAC addresses    : 0
Sticky MAC addresses        : 0
Security violation count    : 0
```

run clear port-security port-error

When the port security violation mode is **shutdown**, the port will be set to the *error-discard* state when detecting a violation. User can recover the port with the **run clear port-security port-error** command.

Command Syntax

run clear port-security port-error interface {**all | gigabit-ethernet** <*interface-name*>}

Parameter

Parameter	Description
interface {**all	gigabit-ethernet** <*interface-name*>}	Specifies the physical interface name.

Example

- Run the command **run clear port-security port-error** to recover the port ge-1/1/33.

```
admin@Xorplus# run clear port-security port-error interface gigabit-ethernet ge-1/1/33
Clear done.
```

run clear port-security sticky interface

The **run clear port-security sticky interface** command clears the sticky secure MAC addresses of a secure interface.

Command Syntax

run clear port-security sticky interface {**all | gigabit-ethernet** <*interface-name*> [**vlan** <*vlan-id*>]}

Parameter

Parameter	Description
interface {**all	gigabit-ethernet** <*interface-name*>}	Specifies the physical interface name. The value could **all** or a specific interface name.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security sticky interface** to clear the sticky secure MAC addresses of ge-1/1/33.

```
admin@Xorplus# run clear port-security sticky interface gigabit-ethernet ge-1/1/33
Clear done.
```

run clear port-security sticky address

The **run clear port-security sticky address** command clears a sticky secure MAC address.

Command Syntax

run clear port-security sticky address <*mac-addr*> [**vlan** <*vlan-id*>*]*

Parameter

Parameter	Description
address <*mac-addr*>	Specifies a secure MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security sticky address** to clear a sticky secure MAC address.

```
admin@Xorplus# run clear port-security sticky address 00:00:0a:00:00:01
Clear done.
```

run clear port-security dynamic interface

The **run clear port-security dynamic interface** command clears the dynamic secure MAC addresses of a secure interface.

Command Syntax

run clear port-security dynamic interface {**all | gigabit-ethernet** <*interface-name*> [**vlan** <*vlan-id*>]}

Parameter

Parameter	Description
interface {**all	gigabit-ethernet** <*interface-name*>}	Specifies the physical interface name. The value could **all** or a specific interface name.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security dynamic interface** to clear the dynamic secure MAC addresses of ge-1/1/33.

```
admin@Xorplus# run clear port-security dynamic interface gigabit-ethernet ge-1/1/33
Clear done.
```

run clear port-security dynamic address

The **run clear port-security dynamic address** command clears a dynamic secure MAC address.

Command Syntax

run clear port-security dynamic address <*mac-addr*> [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
address <*mac-addr*>	Specifies a secure MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers.
vlan <*vlan-id*>	Optional. Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Run the command **run clear port-security dynamic address** to clear a dynamic secure MAC address.

```
admin@Xorplus# run clear port-security dynamic address 00:00:0a:00:00:01
Clear done.
```

L3 Interface

- set l3-interface vlan-interface vrf
- set l3-interface vlan-interface address prefix-length
- set l3-interface loopback address
- set l3-interface loopback disable
- set l3-interface loopback vrf
- set l3-interface vlan-interface rate-limit
- set l3-interface vlan-interface mtu
- set l3-interface vlan-interface dhcp
- run show l3-interface vlan-interface
- run show l3-interface
- run show l3-interface loopback
- run clear l3-interface statistics
- set l3-interface routed-interface dhcp
- set l3-interface routed-interface rate-limit
- set l3-interface routed-interface mtu
- set l3-interface routed-interface vrf
- set l3-interface routed-interface address
- set l3-interface routed-interface description
- run show l3-interface routed-interface
- set l3-interface vlan-interface pmtu-discovery
- set l3-interface routed-interface pmtu-discovery

set l3-interface vlan-interface vrf

The **set l3-interface vlan-interface vrf** command is used to bind the Layer 3 VLAN interface to the VRF.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **vrf** <*vrf-name*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies a Layer 3 VLAN interface. The value is a string.
vrf <*vrf-name*>	Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

By binding the Layer 3 VLAN interfaces to different VRFs, the system segregates the IP routing table, ARP table, hardware forwarding table and host hardware forwarding table of different VRFs in customer edge devices.

Note that: The Layer 3 VLAN interface is in the default VRF if not explicitly bound to any VRF.

Example

- Bind the Layer 3 VLAN interface VLAN10 to the VRF vrf1.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 vrf vrf1
admin@Xorplus# commit
```

set l3-interface vlan-interface address prefix-length

To configure an IPv4 or IPv6 address for an L3 interface, use the **set l3-interface vlan-interface address prefix-length** command in L2/L3 configuration mode. To remove an L3 interface, use the **delete** form of the command.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>
delete l3-interface vlan-interface <*interface-name*>

Parameters

Parameter	Description
vlan-interface <*interface-name*>	Interface name.
address	IPv4 or IPv6 address.
number	The network prefix length. The range is 4-32 for IPv4 addresses, and 1-128 for IPv6 addresses.

Example

- The following example configures the IPv4 address for the *vlan10* L3 interface and then removes the L3 interface:

```
admin@Switch# set l3-interface vlan-interface vlan10 address 192.168.1.1 prefix-length 24
admin@Switch# commit
admin@Switch# delete l3-interface vlan-interface vlan10
```

- The following example configures the IPv6 address for the *vlan20* L3 interface and then removes the L3 interface:

```
admin@Switch# set l3-interface vlan-interface vlan20 address 2001:1:1::1 prefix-length 64
admin@Switch# commit
admin@Switch# delete l3-interface vlan-interface vlan20
```

set l3-interface loopback address

The **set l3-interface loopback address** command creates a loopback interface and configures its IP address.

Command Syntax

set l3-interface loopback <*loopback-name*> **address** <*ip-address*> **prefix-length** <*int*>

Parameters

Parameter	Description
loopback <*loopback-name*>	Specifies a loopback interface. The value is a string.
address <*ip-address*>	Specifies the IP address of a loopback interface. • Ipv4 default value: 127.0.0.1 • Ipv6 default value: ::1
prefix-length <*int*>	The IPv4 network prefix length is fixed to 32. The IPv6 network prefix length is fixed to 128.

Usage Guidelines

A loopback interface is always Up.

The IP address of a loopback interface is usually specified as the source address of packets.

After a loopback interface is created, you can use command **set l3-interface loopback vrf** to bind the loopback interface to a VRF. Users can configure multiple loopback interfaces per VRF. A loopback interface is in the default VRF by default.

You can also use command **set l3-interface loopback disable** to disable a loopback interface. When a loopback interface is created, it is enabled by default.

Note that **lo** is a built-in loopback interface in default VRF, it cannot be bound to any other user-defined VRF, or be disabled.

Example

- Create a loopback interface **lo-gre** in the default VRF.

```
admin@Xorplus# set l3-interface loopback lo-gre address 1.1.1.1 prefix-length 32
admin@Xorplus# commit
```

set l3-interface loopback disable

The **set l3-interface loopback disable** command can be used to enable or disable a loopback interface.

Command Syntax

set l3-interface loopback <*interface-name*> **disable** <**true | false**>

Parameters

Parameter	Description
loopback <*interface-name*>	Specifies the name of the loopback interface. The value is a string.
disable <**true	false**>	Enables or disables the loopback interface. The value could be **true** or **false**. • **true**: Disable the loopback interface. • **false**: Enable the loopback interface. When a loopback interface is created, it is enabled by default.

Example

- Disable loopback interface lo2.

```
admin@Xorplus# set l3-interface loopback lo2 disable true
admin@Xorplus# commit
```

set l3-interface loopback vrf

The **set l3-interface loopback vrf** command can be used to bind the loopback interface to a VRF. Multiple loopback interfaces can be configured within a user configured VRF or the default VRF.

Command Syntax

set l3-interface loopback <*interface-name*> **vrf** <*vrf-name*>

Parameters

Parameter	Description
loopback <*interface-name*>	Specifies the name of the loopback interface. The value is a string.
vrf <*vrf-name*>	Specifies the name of the VRF for the loopback interface.

Example

- Bind the loopback interface lo2 to vrf2.

```
admin@Xorplus# set l3-interface loopback lo2 vrf vrf2
admin@Xorplus# commit
```

set l3-interface vlan-interface rate-limit

The **set l3-interface vlan-interface rate-limit** command configures the CPU egress rate limit for an L3 VLAN interface.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **rate-limit** <*rate-limit*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies a Layer 3 VLAN interface. The value is a string.
rate-limit <*rate-limit*>	Specifies an egress rate limit for the L3 VLAN interface. The value is an integer, in kbps, that ranges from 1 to 1000000000. By default, there is no rate limit for the L3 VLAN interface in the outbound direction.

Usage Guidelines

L3 VLAN interface rate limit is applied to packets delivered out from the CPU, controlling shock of large flow on CPU, releasing the burden on CPU.

Example

- Configure rate limit for the L3 VLAN interface vlan200.

```
admin@Xorplus# set l3-interface vlan-interface vlan200 rate-limit 1024
admin@Xorplus# commit
```

set l3-interface vlan-interface mtu

The **set l3-interface vlan-interface mtu** command configures the maximum transmission unit (MTU) of a Layer 3 VLAN interface.

> **NOTE:**
> The MTU value takes effect only on the outbound interface of the Layer 3 VLAN interface.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **mtu** <*mtu-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a Layer 3 VLAN interface. The value is a string.
mtu <*mtu-value*>	Specifies the MTU of an interface. The value is an integer that ranges from 68 to 65535, in bytes. The default value is 1500 bytes.

Usage Guidelines

An MTU value determines the maximum number of bytes in the IP layer packet that can be sent at a time. If the size of the data packets of the IP layer packet exceeds the MTU supported by a transit node or a receiver, the data packet is dropped at the sender's IP layer.

Example

- Configure the MTU of the VLAN interface vlan10 as 2000.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 mtu 2000
```

set l3-interface vlan-interface dhcp

DHCP can be enable or disable on this VLAN interface as dhcp client. The VLAN interface will get ip address by DHCP server if DHCP is enable on this VLAN interface.

Command Syntax
set l3-interface vlan-interface <*interface-name*> **dhcp** <*boolean*>

Parameter
•<*interface-name*> *Vlan interface name is defined*.
•<*boolean*> *enable or disable dhcp on vlan-interface as client*. The value include:

- **true** Enable DHCP client on this vlan interface.
- **False** Default configuration. Disable DHCP client on this VLAN interface.

Example

- This example manually enables DHCP on the VLAN interface.

```
admin@XorPlus#set l3-interface vlan-interface vlan2 dhcp true
admin@XorPlus# commit
```

run show l3-interface vlan-interface

To display information about an L3 VLAN interface, use the **run show l3-interface vlan-interface** command in L2/L3 configuration mode.

Command Syntax

run show l3-interface vlan-interface <*interface-name*> [**detail**]

Parameters

Parameter	Description
interface-name	Optional. The VLAN interface name.
detail	Optional. Show detail informations of all VLAN interface.

Example

- The following example displays information about **vlan10**:

```
admin@Switch# run show l3-interface vlan-interface vlan10
vlan10      Hwaddr E0:07:1B:C9:20:9B, Vlan:10, MTU: 1450, State:UP
            Inet addr: 10.1.1.166/24
                       fe80::e207:1b20:1c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.........................0
              IPv4 Forwarding Packets....................0
              IPv6 Input Packets.........................0
              IPv6 Forwarding Packets....................0
```

- The following example displays the detail information about **vlan10**:

```
admin@Switch# run show l3-interface vlan-interface vlan10 detail
vlan10      Hwaddr E0:07:1B:C9:20:9B, Vlan:10, MTU: 1450, State:UP
            Inet addr: 10.1.1.166/24
                       fe80::e207:1b20:1c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.........................0
              IPv4 Forwarding Packets....................0
              IPv6 Input Packets.........................0
              IPv6 Forwarding Packets....................0
            Port        State         Tag
            ----------  ------------  --------
            te-1/1/1    FORWARDING    tagged
            te-1/1/17   DOWN          tagged
            te-1/1/2    FORWARDING    tagged
```

run show l3-interface

To display information about all L3 interfaces, use the **run show l3-interface** command in L2/L3 configuration mode.

Command Syntax

run show l3-interface [brief | detail]

Parameters

Parameter	Description
brief	Optional. Show all L3 interfaces briefly.
detail	Optional. Show detail information of all L3 interfaces.

Example

- The following example displays information about all L3 interfaces.

```
admin@Switch# run show l3-interface
lo          Hwaddr E0:07:1B:C9:20:9B, Vlan:4095, MTU: 1500, State:UP
            Inet addr: fe80::e207:1b20:c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets.....................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets.....................0

vlan10      Hwaddr E0:07:1B:C9:20:9B, Vlan:10, MTU: 1450, State:UP
            Inet addr: 10.1.1.166/24
                       fe80::e207:1b20:1c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets.....................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets.....................0

vlan100     Hwaddr E0:07:1B:C9:20:9B, Vlan:100, MTU: 1500, State:DOWN
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.....................0
              IPv4 Forwarding Packets.....................0
              IPv6 Input Packets.....................0
              IPv6 Forwarding Packets.....................0
```

- This example shows all L3 interfaces briefly:

```
admin@XorPlus# run show l3-interface brief
Interface    Vlan ID    Status    Addr
---------    -------    ------    ------------------
lo           4095       UP        fe80::e207:1b20:c9:209b/64
vlan10       10         UP        10.1.1.166/24
                                  fe80::e207:1b20:1c9:209b/64
vlan100      100        DOWN
vlan1000     1000       UP        10.1.1.166/24
```

```
                    fe80::e207:1b20:8c9:209b/64
```

run show l3-interface loopback

To display information about a L3 VLAN interface or loopback interface, use the **run show l3-interface loopback** command in L2/L3 configuration mode.

Command Syntax

run show l3-interface loopback {**lo** | *<vrf-name>*}

Parameters

Parameter	Description
{**lo** | *<vrf-name>*}	Required parameter. Specifies VRF name. • **lo**: indicates the loopback interface in default VRF. • *<vrf-name>:* Specifies VRF name. The value is a string.

Example

- The following example displays information about the loopback interface in the default VRF:

```
admin@Switch# run show l3-interface loopback lo
lo          Hwaddr E0:07:1B:C9:20:9B, Vlan:4095, MTU: 1500, State:UP
            Inet addr: fe80::e207:1b20:c9:209b/64
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.........................0
              IPv4 Forwarding Packets....................0
              IPv6 Input Packets.........................0
              IPv6 Forwarding Packets....................0
```

run clear l3-interface statistics

This command clears the statistics information of L3 interface.

Command Syntax

run clear l3-interface statistics [**loopback** | <*vlan-interface*>]

Parameters

Parameter	Description
[**loopback** | <*vlan-interface*>]	Specifies the loopback interface or a VLAN interface.

Example

• This example clears the statistics information of loopback interface:

```
admin@XorPlus# run clear l3-interface statistics loopback
admin@XorPlus# commit
```

set l3-interface routed-interface dhcp

DHCP can be enable or disable on this routed interface or sub-interface as dhcp client. The routed interface or sub-interface will get ip address by DHCP server if DHCP is enable on this interface.

Command Syntax
set l3-interface routed-interface <*interface-name*> **dhcp** <*boolean*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
dhcp <*boolean*>	Enables or disables DHCP on a routed interface or sub-interface as DHCP client. The value include: • **true:** Enable DHCP client on routed interface or sub-interface. • **false:** Default configuration. Disable DHCP client on routed interface or sub-interface.

Example

- Enable DHCP client on routed interface.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 dhcp true
admin@XorPlus# commit
```

set l3-interface routed-interface rate-limit

The **set l3-interface routed-interface rate-limit** command configures the CPU egress rate limit for an L3 VLAN interface.

The **delete l3-interface routed-interface rate-limit** command deletes the CPU egress rate limit for a routed interface or a sub-interface.

Command Syntax

set l3-interface routed-interface <*interface-name*> **rate-limit** <*rate-limit*>

delete l3-interface routed-interface <*interface-name*> **rate-limit**

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
rate-limit <*rate-limit*>	Specifies an egress rate limit for the L3 VLAN interface. The value is an integer, in kbps, that ranges from 1 to 1000000000. By default, there is no rate limit for the L3 VLAN interface in the outbound direction.

Usage Guidelines

Routed interface rate limit is applied to packets delivered out from the CPU, controlling shock of large flow of packets and releasing the burden on CPU.

Example

- Configure rate limit for a routed interface.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 rate-limit 1024
admin@Xorplus# commit
```

set l3-interface routed-interface mtu

The **set l3-interface routed-interface mtu** command configures the maximum transmission unit (MTU) of a Layer 3 routed interface.

The **delete l3-interface routed-interface mtu** command deletes the IP MTU to the default value.

NOTE:

- The MTU value takes effect only on the outbound interface of the routed interface.
- It is not supported to configure MTU on the sub-interfaces. The sub-interfaces use the MTU value configured on the parent interface.
- If you need to use IPv6 related functions, MTU needs at least 1280 bytes.

Command Syntax

set l3-interface routed-interface <*interface-name*> **mtu** <*mtu-value*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name. The value is a string.
mtu <*mtu-value*>	Specifies the MTU of an interface. The value is an integer that ranges from 68 to 65535, in bytes. The default value is 1500 bytes.

Usage Guidelines

An MTU value determines the maximum number of bytes in the IP layer packet that can be sent at a time. If the size of the data packets of the IP layer packet exceeds the MTU supported by a transit node or a receiver, the data packet is dropped at the sender's IP layer.

Example

- Configure the MTU for a routed interface.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 mtu 2000
admin@Xorplus# commit
```

set l3-interface routed-interface vrf

The **set l3-interface routed-interface vrf** command is used to bind the layer 3 routed interface or sub-interface to the VRF.

Command Syntax

set l3-interface routed-interface<*interface-name*> **vrf** <*vrf-name*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
vrf <*vrf-name*>	Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

By binding the routed interfaces or sub-interfaces to different VRFs, the system segregates the IP routing table, ARP table, hardware forwarding table and host hardware forwarding table of different VRFs in customer edge devices.

Note that: The routed interfaces or sub-interfaces are in the default VRF if not explicitly bound to any VRF.

Example

• Bind the routed interface *rif-te4* to the VRF *vrf1*.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 vrf vrf1
admin@Xorplus# commit
```

set l3-interface routed-interface address

To configure an IPv4 or IPv6 address for an L3 interface, use the **set l3-interface routed-interface address** command in L2/L3 configuration mode. To remove an L3 interface, use the **delete** form of the command.

Command Syntax

set l3-interface routed-interface <*interface-name*> **address** <*address*> **prefix-length** <*number*>
delete l3-interface routed-interface <*interface-name*>

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
address	IPv4 or IPv6 address.
number	The network prefix length. The range is 4-32 for IPv4 addresses, and 1-128 for IPv6 addresses.

Usage Guidelines

Layer 3 interfaces, including VLAN interface, loopback interface, routed interface and sub- interface, share the same hardware resources. When configuring IP address, it is required that the IP addresses of different layer 3 interfaces in the same VRF cannot be in the same subnet; However, overlapped layer 3 interface addresses in different VRFs is supported.

Example

- Configure the IPv4 address for a routed interface.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# set l3-interface routed-interface rif-te4 address 10.10.0.1 prefix-length 24
admin@Xorplus# commit
```

- The following example configures the IPv6 address for the routed interface and then removes the L3 interface:

```
admin@Switch# set l3-interface routed-interface rif-te5 address 2001:1:1::1 prefix-length 64
admin@Switch# commit
admin@Switch# delete l3-interface routed-interface rif-te5
```

set l3-interface routed-interface description

The **set l3-interface routed-interface description** command configures the descriptive information for a routed interface or a sub-interface to help administrators and operators identify the purpose or role of an interface.

The **delete l3-interface routed-interface description** command deletes the descriptive information for a routed interface or a sub-interface.

Command Syntax

set l3-interface routed-interface<*interface-name*> **description** <*description*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
description <*description*>	Specifies a description for the interface. The value is a string.

Example

• Configure the description for a routed interface to *west*.

```
admin@Xorplus# set l3-interface routed-interface rif-te4 description west
admin@Xorplus# commit
```

run show l3-interface routed-interface

The **run show routed interface** command shows the detailed layer 3 interface information of a specific routed interface or sub-interface.

Command Syntax

run show l3-interface routed-interface <*interface-name*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.

Example

- View the detailed layer 3 information of a specific routed interface.

```
admin@Xorplus# run show l3-interface routed-interface rif-te1
rif-te1          Hwaddr 18:5A:58:1F:63:A1, Vlan:800, MTU: 1500, State:UP
                 Inet addr: 120:1:1::49/64
                            fe80::1a5a:5820:131f:63a1/64
                 Traffic statistics:
                   5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
                   5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
                   IPv4 Input Packets.............................0
                   IPv4 Forwarding Packets........................0
                   IPv6 Input Packets.............................0
                   IPv6 Forwarding Packets........................0
```

set l3-interface vlan-interface pmtu-discovery

The **set l3-interface vlan-interface pmtu-discovery** command is used to enable or disable Path MTU(PMTU) function on a VLAN interface.

> **NOTE**:
> Enable PMTU function on all the nodes in the path where you want to apply the PMTU function.

The **delete l3-interface vlan-interface pmtu-discovery** command deletes the configuration.

Command Syntax

set l3-interface vlan-interface <*vlan-interface*> **pmtu-discovery disable** <**true | false**>

Parameters

Parameter	Description
vlan-interface <*vlan-interface*>	Specifies the Layer 3 VLAN interface name. The value is a string.
disable <true | false>	Enables or disables the PMTU function. The value is **true** or **false**. • **true**: disables the PMTU function. • **false**: enables the PMTU function. By default, PMTU function is disabled.

Example

- Enable PMTU function on VLAN interface *vlan100*.

```
admin@PICOS# set l3-interface vlan-interface vlan100 pmtu-discovery disable false
admin@PICOS# commit
```

set l3-interface routed-interface pmtu-discovery

The **set l3-interface routed-interface pmtu-discovery** command is used to enable or disable Path MTU(PMTU) function on a routed interface.

> **NOTE**:
> Enable PMTU function on all the nodes in the path where you want to apply the PMTU function.

The **delete l3-interface routed-interface pmtu-discovery** command deletes the configuration.

Command Syntax

set l3-interface routed-interface <*routed-interface*> **pmtu-discovery disable** <**true | false**>

Parameters

Parameter	Description
routed-interface <*routed-interface*>	Specifies the Layer 3 routed interface name. The value is a string.
disable <true | false>	Enables or disables the PMTU function. The value is **true** or **false**. • **true**: disables the PMTU function. • **false**: enables the PMTU function. By default, PMTU function is disabled.

Example

- Enable PMTU function on routed interface *rif-te19*.

```
admin@PICOS# set l3-interface routed-interface rif-te19 pmtu-discovery disable false
admin@PICOS# commit
```

Routed Interface

- run show interface routed-interface brief
- run show vlans routed-vlan
- set interface aggregate-ethernet routed-interface enable
- set interface aggregate-ethernet routed-interface name
- set interface aggregate-ethernet routed-interface sub-interface vlan-id
- set interface gigabit-ethernet routed-interface enable
- set interface gigabit-ethernet routed-interface sub-interface
- set vlans reserved-vlan
- set interface gigabit-ethernet routed-interface name

run show interface routed-interface brief

The **run show interface routed-interface brief** command shows the brief information of the routed interfaces and sub-interfaces.

Command Syntax

run show interface routed-interface brief

Parameter

Null.

Example

- View the configuration information of routed interfaces and sub-interfaces.

```
admin@Xorplus# run show interface routed-interface brief
Interface       RoutedIfName     SubRoutedIfName  VLANID  Management  Status  Flow Control  Duplex  Speed    Descri
--------------  ---------------  ---------------  ------  ----------  ------  ------------  ------  -------  ------
te-1/1/1        rif-1                             800     Enabled     Up      Disabled      Full    1Gb/s
                                 rif-1.1          1102
                                 rif-1.2          1100
                                 rif-1.3          1101
te-1/1/2        rif-te2                           801     Disabled    Down    Disabled      Full    Auto
te-1/1/4        rif-te4                           802     Enabled     Down    Disabled      Full    Auto
te-1/1/5        rif-2                             803     Enabled     Up      Disabled      Full    2.5Gb/s
```

run show vlans routed-vlan

The **run show vlans routed-vlan** command shows the VLAN information of the routed interfaces and sub-interfaces.

Command Syntax

run show vlans routed-vlan

Parameter

Null.

Example

- View the VLAN information of the routed interfaces and sub-interfaces.

```
admin@Xorplus# run show vlans routed-vlan
VlanID  Vlan Name           Tag         Interfaces     Routed-interfaces
------  ------------------  --------    ------------   --------------------
800                         untagged    ge-1/1/5       rif-1
801                         untagged    ge-1/1/7       rif-2
1100    default             tagged      ge-1/1/5       rif-1.2
1101    default             tagged      ge-1/1/5       rif-1.3
1102    default             tagged      ge-1/1/5       rif-1.1
1103    default             tagged      ge-1/1/7       rif-2.1
```

The field “**Tag**” indicates whether the packets will be tagged or not when they are sent from this port.

set interface aggregate-ethernet routed-interface enable

The **set interface aggregate-ethernet routed-interface enable** command enables a LAG port as a layer 3 routed interface. LAG ports are layer 2 interfaces by default.

The **delete interface aggregate-ethernet routed-interface enable** command restores the LAG port to a layer 2 interface.

Command Syntax

set interface aggregate-ethernet <*lag-name*> **routed-interface enable <true | false>**

Parameter

Parameter	Description
aggregate-ethernet <*lag-name*>	Specifies the name of a LAG port. The value is like ae1, ae10, etc.
enable <true | false>	Enables or disables the LAG port as a layer 3 routed interface. The value could be **true** or **false**. • **true**: Enables the LAG port as a layer 3 routed interface. • **false**: Disables the LAG port as a layer 3 routed interface. All LAG ports are layer 2 interfaces by default.

Example

- Enable the LAG port *ae3* as a layer 3 routed interface.

```
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface enable true
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface name rif-ae3
admin@Xorplus# commit
```

set interface aggregate-ethernet routed-interface name

The **set interface aggregate-ethernet routed-interface name** command configures the name for the routed interface, which will be referred to in other CLI commands as the routed interface name.

Command Syntax

set interface aggregate-ethernet <*lag-name*> **routed-interface name** <*string*>

Parameter

Parameter	Description
aggregate-ethernet <*lag-name*>	Specifies the name of a LAG port. The value is like ae1, ae10, etc.
name <*string*>	Specifies the name for the routed interface. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

Example

- Configure the name for the routed interface.

```
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface enable true
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface name rif-ae3
admin@Xorplus# commit
```

set interface aggregate-ethernet routed-interface sub-interface vlan-id

The **set interface aggregate-ethernet routed-interface sub-interface vlan-id** command creates a sub-interface and adds it into a VLAN. When creating a sub-interface, VLAN ID needs to be specified at the same time.

Command Syntax

set interface aggregate-ethernet <*lag-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

Parameter

Parameter	Description
aggregate-ethernet <*lag-name*>	Specifies the name of a LAG port. The value is like ae1, ae10, etc.
sub-interface <sub-interface-name>	Specifies the sub-interface name. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.
vlan-id <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 2 to4094.

Example

- Create a sub-interface and add to VLAN 10.

```
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface enable true
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface name rif-ae3
admin@Xorplus# set interface aggregate-ethernet ae3 routed-interface sub-interface rif-ae3.1 vlan-id 10
admin@Xorplus# commit
```

set interface gigabit-ethernet routed-interface enable

The **set interface gigabit-ethernet routed-interface enable** command enables the Ethernet port as a layer 3 routed interface. All Ethernet ports are layer 2 interfaces by default.

The **delete interface gigabit-ethernet routed-interface enable** command restores the Ethernet port to a layer 2 interface.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **routed-interface enable <true | false>**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3, etc.
enable <true | false>	Enables or disables the Ethernet port as a layer 3 routed interface. The value could be **true** or **false**. • **true**: Enables the Ethernet port as a layer 3 routed interface. • **false**: Disables the Ethernet port as a layer 3 routed interface. All Ethernet ports are layer 2 interfaces by default.

Usage Guidelines

Pay attention to the following precautions before configuring a routed interface:

When enabling an Ethernet port/LAG interface as a layer 3 routed interface, a name for the routed interface should be configured by using the command **set interface gigabit-ethernet** <*interface-name*> **routed-interface name** <*string*>. This name will be referred to as the “interface name” in other CLI commands.

> **NOTE:**
> To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

Reserved VLANs need to be configured on the device before configuring the routed interface.

Routed interface is mutually exclusive with the following layer 2 features, you have to delete all of the following configurations on the interface before enabling it as a routed interface, otherwise the routed interface commands will fail to commit.

set interface gigabit-ethernet <*interface-name*> **backup-port** *XX*
set interface aggregate-ethernet <*lag-name*> **backup-port** *XX*
set interface gigabit-ethernet <*interface-name*> **crossflow** *XX*
set interface aggregate-ethernet <*lag-name*> **crossflow** *XX*
set interface gigabit-ethernet <*interface-name*> **family** *XX*
set interface aggregate-ethernet <*lag-name*> **family** *XX*
set interface gigabit-ethernet <*interface-name*> **loopback true**
set interface gigabit-ethernet <*interface-name*> **port-security** *XX*
set interface aggregate-ethernet <*lag-name*> **port-security** *XX*
set interface gigabit-ethernet <*interface-name*> **static-ethernet-switching mac-address** *XX*
set interface aggregate-ethernet <*lag-name*> **static-ethernet-switching mac-address** *XX*
set interface gigabit-ethernet <*interface-name***> voice-vlan** *XX*
set interface aggregate-ethernet <*lag-name*> **voice-vlan** *XX*
set protocols dhcp snooping trust-port <*trust-port*>
set protocols igmp-snooping vlan-id <*vlan-id*> **mrouter interface** <*interface-name*>
set protocols igmp-snooping vlan-id <*vlan-id*> **static group** <*group-address*> **interface** <*interface-name*>
set protocols dot1x interface <*interface-name*>
set interface gigabit-ethernet <*interface-name*> **breakout true**

Besides the layer 2 features listed above, routed interface does not support Spanning Tree Protocol (STP) and MAC learning. However, the Layer 2 feature of LLDP is supported on an Ethernet port enabled as routed interface.

After a routed interface is enabled, you have to configure the following node to bring the routed interface up. Only after this, the corresponding sub-interfaces can be used normally.

set l3-interface routed-interface <*interface-name*>

The member port of a LAG port cannot be enabled as a routed interface, correspondingly, the physical port enabled as a routed interface cannot be configured as a LAG member port.

Example

- Enable the Ethernet port te-1/1/4 as a layer 3 routed interface.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# commit
```

set interface gigabit-ethernet routed-interface sub-interface

The **set interface gigabit-ethernet routed-interface sub-interface** command creates a sub-interface. When creating a sub-interface, VLAN ID needs to be specified at the same time.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **routed-interface sub-interface** <*sub-interface-name*> **vlan-id** <*vlan-id*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3, etc.
sub-interface <*sub-interface-name*>	Specifies the sub-interface name. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.
vlan-id <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 2 to 4094.

Usage Guidelines

Pay attention to the following precautions before configuring the sub-interfaces:

- Enable the Ethernet port as a routed interface before configuring the sub-interfaces.
- Define the VLAN ID by using the command **set vlans vlan-id** <*vlan-id*> before configuring the sub-interface and adding to VLAN.
- The IP address for each sub-interface should be in a different subnet from all the other sub-interfaces under that parent interface. That is, the IP subnets of all the sub-interfaces should be unique under the same parent interface.
- It is not supported to configure MTU on the sub-interfaces. The sub-interfaces use the MTU value configured on the parent interface.
- On greyhound2 switches (including Dell N22xx series switches and N3208PX-ON), the sub-interface does not support user defined VRF and can only be used in the default VRF.
- The sub-interface of LAG port does not support user defined VRF and can only be used in the default VRF.

Example

- Create a sub-interface and add to VLAN 10.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface sub-interface rif-te4.1 vlan-id 10
admin@Xorplus# commit
```

set vlans reserved-vlan

The **set vlans reserved-vlan** command configures reserved VLANs for the use of routed interfaces.

Command Syntax

set vlans reserved-vlan <*reserved-vlan*>

Parameter

Parameter	Description
reserved-vlan <*reserved-vlan*>	Specifies the reserved VLANs. The valid VLAN numbers range is 2-4094. User can specify a range of VLAN numbers, e.g. 2,3,50-100. The system supports up to 128 reserved VLANs.

Usage Guidelines

Whenever a routed interface is configured, the system will automatically assign a VLAN internally to the routed interface from the reserved VLANs in order of smallest to largest.

The system supports up to 128 reserved VLANs.

VLAN 1 cannot be used as a reserved VLAN.

A reserved VLANs are VLANs dedicated to the routed interfaces (sub-interfaces are not included) and cannot be used for other interfaces, or other VLAN functions, such as PVLAN.

Reserved VLAN is mutually exclusive with the following settings, before configuring, please delete all these commands that uses the reserved VLAN, otherwise the reserved VLAN command will fail to commit.

set protocols dhcp snooping vlan <*vlan-id*>
set protocols igmp-snooping vlan-id <*vlan-id*>
set protocols dot1x block-vlan-id <*vlan-id*>
set protocols dot1x server-fail-vlan-id <*vlan-id*>
set vlans vlan-id <*vlan-id*> **private-vlan** *XX*

Note that: If you want to modify the value of the reserved VLANs, all the routed interfaces need to be disabled first.

You can use the commands **run show vlans** and **run show vlans routed-vlan** to check the VLAN information of all routed interfaces. For example,

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/2 routed-interface name rif-te2
admin@Xorplus# set interface gigabit-ethernet te-1/1/2 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set vlans reserved-vlan 80-85
admin@Xorplus# commit

admin@Xorplus# run show vlans
VlanID  Vlan Name           Tag        Interfaces
------  -----------------  --------   ------------------------------------------------------
1       default            untagged   te-1/1/1, xe-1/1/1, xe-1/1/2, xe-1/1/3, te-1/1/3
                                      xe-1/1/4, xe-1/1/5, te-1/1/5, xe-1/1/6, te-1/1/6
                                      te-1/1/7, te-1/1/8, te-1/1/9, te-1/1/10, te-1/1/11
                                      te-1/1/12, te-1/1/13, te-1/1/14, te-1/1/15, te-1/1/16
                                      te-1/1/17, te-1/1/18, te-1/1/19, te-1/1/20, te-1/1/21
                                      te-1/1/22, te-1/1/23, te-1/1/24, te-1/1/25, te-1/1/26
                                      te-1/1/27, te-1/1/28, te-1/1/29, te-1/1/30, te-1/1/31
                                      te-1/1/32, te-1/1/33, te-1/1/34, te-1/1/35, te-1/1/36
                                      te-1/1/37, te-1/1/38, te-1/1/39, te-1/1/40, te-1/1/41
                                      te-1/1/42, te-1/1/43, te-1/1/44, te-1/1/45, te-1/1/46
                                      te-1/1/47, te-1/1/48
                           tagged

80                         untagged   te-1/1/2
                           tagged
```

```
81                      untagged   te-1/1/4
                        tagged

82                      untagged
                        tagged

83                      untagged
                        tagged

84                      untagged
                        tagged

85                      untagged
                        tagged

admin@Xorplus# run show vlans routed-vlan
VlanID  Vlan Name           Tag         Interfaces     Routed-interfaces
------  ------------------  --------    ------------   --------------------
80                      untagged    te-1/1/2        rif-te2
81                      untagged    te-1/1/4        rif-te4
```

Example

- Configure reserved VLANs for the use of routed interfaces.

```
admin@Xorplus# set vlans reserved-vlan 800-900
admin@Xorplus# commit
```

set interface gigabit-ethernet routed-interface name

The **set interface gigabit-ethernet routed-interface name** command configures the name for the routed interface, which will be referred to in other CLI commands as the routed interface name.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **routed-interface name** <*string*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3, etc.
name <*string*>	Specifies the name for the routed interface. The value could be up to 15 alphanumeric characters (including three special characters . – and @). **NOTE**: To avoid conflict with the preserved interface names, the routed interface name and sub-interface name must start with the string "**rif-**". Otherwise, commit will fail with the error message "*The name of interface must start with "rif-"*.

Example

- Configure the name for the routed interface.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface enable true
admin@Xorplus# set interface gigabit-ethernet te-1/1/4 routed-interface name rif-te4
admin@Xorplus# commit
```

Uplink Failure Detection Commands

- run show interface ufd
- set interface ufd link-to-monitor
- set interface ufd link-to-disable

run show interface ufd

The **run show interface ufd** command is used to view the uplink failure detection configuration information and status.

Command Syntax

run show interface ufd

Parameter

None.

Example

- View uplink failure detection configuration information and status.

```
admin@Xorplus# run show interface ufd
UFD: ufd1
-----------------------------------------------------
Uplink        : te-1/1/1 te-1/1/24
Downlink      : te-1/1/2 te-1/1/3
Failure Action: Inactive

UFD: ufd10
-----------------------------------------------------
Uplink        : te-1/1/10
Downlink      : te-1/1/11
Failure Action: Active
```

- If both the uplink and downlink interfaces are down, then the status of *Failure Action* is **Active** in the output. It means that uplink failure detection is working.
- If there is an uplink that is up, and hence that the downlink interface is also up, and that the status of *Failure Action* is **Inactive**.

set interface ufd link-to-monitor

The **set interface ufd link-to-monitor** command configures the uplink interface to an uplink failure detection group.

The **delete interface ufd link-to-monitor** command deletes the configuration.

Command Syntax

set interface ufd <*ufd-group-name*> **link-to-monitor** <*interface-name*>

Parameter

Parameter	Description
ufd <*ufd-group-name*>	Specifies the UFD group name. The value is a string in alpha-numeric format with no spaces.
link-to-monitor <*interface-name*>	Specifies the uplink interface to a UFD group. The value is a physical interface or a LAG interface.

Example

- Configure the uplink interface to an uplink failure detection group.

```
admin@Xorplus# set interface ufd ufd1 link-to-monitor ge-1/1/2
admin@Xorplus# commit
```

set interface ufd link-to-disable

The **set interface ufd link-to-disable** command configures the downlink interface to an uplink failure detection group.

The **delete interface ufd link-to-disable** command deletes the configuration.

Command Syntax

set interface ufd <*ufd-group-name*> **link-to-disable** <*interface-name*>

Parameter

Parameter	Description
ufd <*ufd-group-name*>	Specifies the UFD group name. The value is a string in alpha-numeric format with no spaces.
link-to-disable <*interface-name*>	Specifies the downlink interface to a UFD group. The value is a physical interface or a LAG interface.

Example

- Configure the downlink interface to an uplink failure detection group.

```
admin@Xorplus# set interface ufd ufd1 link-to-disable ge-1/1/3
admin@Xorplus# commit
```

IPv6 Neighbor Discovery Protocol Command Reference

This section describes the PICOS IPv6 Neighbor Discovery configuration commands.

> Please note that the N22XX series switches do not support IPv6.

- set l3-interface routed-interface ipv6-nd adv-interval-option
- set l3-interface routed-interface ipv6-nd home-agent-config-flag
- set l3-interface routed-interface ipv6-nd home-agent-lifetime
- set l3-interface routed-interface ipv6-nd home-agent-preference
- set l3-interface routed-interface ipv6-nd managed-config-flag
- set l3-interface routed-interface ipv6-nd mtu
- set l3-interface routed-interface ipv6-nd other-config-flag
- set l3-interface routed-interface ipv6-nd prefix off-link
- set l3-interface routed-interface ipv6-nd prefix preferred-lifetime
- set l3-interface routed-interface ipv6-nd prefix router-address
- set l3-interface routed-interface ipv6-nd prefix valid-lifetime
- set l3-interface routed-interface ipv6-nd ra-fast-retrans
- set l3-interface routed-interface ipv6-nd ra-interval
- set l3-interface routed-interface ipv6-nd ra-lifetime
- set l3-interface routed-interface ipv6-nd reachable-time
- set l3-interface routed-interface ipv6-nd router-preference
- set l3-interface routed-interface ipv6-nd suppress-ra
- set l3-interface vlan-interface ipv6-nd adv-interval-option
- set l3-interface vlan-interface ipv6-nd home-agent-config-flag
- set l3-interface vlan-interface ipv6-nd home-agent-lifetime
- set l3-interface vlan-interface ipv6-nd home-agent-preference
- set l3-interface vlan-interface ipv6-nd managed-config-flag
- set l3-interface vlan-interface ipv6-nd mtu
- set l3-interface vlan-interface ipv6-nd other-config-flag
- set l3-interface vlan-interface ipv6-nd prefix off-link
- set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime
- set l3-interface vlan-interface ipv6-nd prefix router-address
- set l3-interface vlan-interface ipv6-nd prefix valid-lifetime
- set l3-interface vlan-interface ipv6-nd ra-fast-retrans
- set l3-interface vlan-interface ipv6-nd ra-interval
- set l3-interface vlan-interface ipv6-nd ra-lifetime
- set l3-interface vlan-interface ipv6-nd reachable-time
- set l3-interface vlan-interface ipv6-nd router-preference
- set l3-interface vlan-interface ipv6-nd suppress-ra

set l3-interface routed-interface ipv6-nd adv-interval-option

Run the command **set l3-interface routed-interface ipv6-nd adv-interval-option** to include the advertisement interval option in the RA packets. The Advertisement Interval Option indicates to host the maximum time in milliseconds between successive unsolicited Router Advertisements.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd adv-interval-option**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd adv-interval-option**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
adv-interval-option	Indicates the Ra packet advertisement interval option.

Example

- This example includes the advertisement interval option in RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd adv-interval-option
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd home-agent-config-flag

Run the command **set l3-interface routed-interface ipv6-nd home-agent-config-flag** to set or unset the home agent config flag in RA packets. The Home Agent Option flag can be set or unset in IPv6 RA packets and is used to indicate to hosts that the router acts as Home Agent and includes a Home Agent Option. This option is not set by default.

Run the command **delete l3-interface routed-interface ipv6-nd home-agent-config-flag** to unset the flag.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-config-flag**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-config-flag**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
home-agent-config-flag	Indicates the home agent config flag in the RA packet.

Example

- This example command sets the home agent config flag in the RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd home-agent-config-flag
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd home-agent-lifetime

Run the command **set l3-interface routed-interface ipv6-nd home-agent-lifetime** to set the home agent lifetime value in seconds. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the current Router Lifetime value.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-lifetime <***seconds*>

delete l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-lifetime <***seconds*>

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
home-agent-lifetime <*seconds*>	Specifies the home agent lifetime in seconds. The value is an integer that ranges from 0 to 65520. The default value is 0.

Example

- This example configures the home agent lifetime to 5 seconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd home-agent-lifetime 5
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd home-agent-preference

Run the command **set l3-interface routed-interface ipv6-nd home-agent-preference** to configure the home agent preference in RA packets. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the least preferred.

Run the command **delete l3-interface routed-interface ipv6-nd home-agent-preference** to delete this configuration and revert to the default value of 0.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-preference <***preference*>

set l3-interface routed-interface <*interface-name*> **ipv6-nd home-agent-preference <***preference*>

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
home-agent-preference <*preference*>	Specifies the home agent preference. The value is an integer that ranges from 0 to 65535. The default value is 0.

Example

- This example configures the home agent preference to 5.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd home-agent-preference 5
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd managed-config-flag

Run the command **set l3-interface routed-interface ipv6-nd managed-config-flag** to set or unset the managed config flag in the IPv6 RA packets. This flag indicates to the hosts that they must use managed protocol or stateful addresses autoconfiguration besides any addresses autoconfigured using stateless address autoconfiguration.

This flag is not set by default. To delete this configuration or unset the flag, run the command **delete l3-interface routed-interface ipv6-nd managed-config-flag.**

Command Syntax

set l3-interface routed-interface <*interface-name***> ipv6-nd managed-config-flag**

delete l3-interface routed-interface <*interface-name***> ipv6-nd managed-config-flag**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.

Example

- This example sets the managed config flag in the RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd managed-config-flag
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd mtu

Run the command **set l3-interface routed-interface ipv6-nd mtu** to include the MTU option is RA packets. This option assists the hosts in proper interface configuration. The advertised MTU is not verified to be consistent with the actual router interface MTU.

Run the command **delete l3-interface routed-interface ipv6-nd mtu** to delete this option. This value is not configured in RA packets by default.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd mtu <***value*>

delete l3-interface routed-interface <*interface-name*> **ipv6-nd mtu**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
mtu <*value*>	Specifies the MTU value to advertise in RA packets. The value is an integer that ranges from 1 65535.

Example

- This example configures the advertised MTU value to 1000.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd mtu 1000
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd other-config-flag

Run the command **set l3-interface routed-interface ipv6-nd other-config-flag** to set the *other config flag* in RA packets. This flag indicates to hosts that administered or stateful protocol should be used for autoconfiguration information other than addresses. This flag is not set by default.

Run the command **delete l3-interface routed-interface ipv6-nd other-config-flag** to unset this flag in RA packets.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd other-config-flag**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd other-config-flag**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.

Example

- This example sets the *other config flat* in RA packets.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd other-config-flag
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix off-link

Run the command **set l3-interface routed-interface ipv6-nd prefix** to configure an IPv6 prefix to include in RA packets without specifying on-link or off-link properties of the advertised prefix. The off-link option is not set by default which means the prefix can be used for on-link determination. The optional parameter **no-autoconfig** can be used to indicate to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix** <*IPv6 Prefix*> **off-link [no-autoconfig]**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **off-link [no-autoconfig]**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
no-autoconfig	This option indicates to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Example

- This example configures an IPv6 prefix with off-link and no-autoconfig options.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 off-link no-autoconfig
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix preferred-lifetime

Run the command **set l3-interface routed-interface ipv6-nd prefix preferred-lifetime** to configure the advertised prefix preferred lifetime in seconds. Addresses generated from the prefix during this time period will be considered preferred addresses.

Run the command **delete l3-interface routed-interface ipv6-nd prefix preferred-lifetime** to remove this configuration.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix prefix <***IPv6 Prefix*> **preferred-lifetime <***seconds* **| infinite>**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd prefix prefix <***IPv6 Prefix*> **preferred-lifetime**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
preferred-lifetime <*seconds* **| infinite>**	Specifies the time the addresses are treated as preferred addresses. The value could be in seconds from 0 to 4294967295 with default value of 604800 or use keyword **infinite** indicating infinity.

Example

- This example configures an IPv6 prefix with with infinite preferred lifetime.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 preferred-lifetime infinite
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix router-address

Run the command **set l3-interface routed-interface ipv6-nd prefix router-address** to set the R flag to indicate to hosts on local link that the specified prefix contains a complete IP address. This flag is not set by default which means hosts do not assume a complete IP address is placed.

Run the command **delete l3-interface routed-interface ipv6-nd prefix router-address** to unset this flag.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **router-address**

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **router-address**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64.

Example

- This example sets the R flag for the given prefix.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 router-address
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd prefix valid-lifetime

Run the command **set l3-interface routed-interface ipv6-nd prefix valid-lifetime** to configure the time in seconds during which the prefix is considered valid for on-link determination.

Run the command **delete l3-interface routed-interface ipv6-nd prefix valid-lifetime** to delete this configuration and revert to the default value of 2592000 seconds.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **valid-lifetime <***seconds* **| infinite>**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd prefix <***IPv6 Prefix*> **valid-lifetime**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
valid-lifetime <*seconds* **| infinite>**	Specifies the time period for which the prefix is valid. The value could be in seconds, Range: (0-4294967295) Default: 2592000. Or it could be **infinite** indicating infinite time.

Example

- This example configures the valid time of IPv6 prefix to infinity.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd prefix fa00::0/64 valid-lifetime infinite
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd ra-fast-retrans

Run the command **set l3-interface routed-interface ipv6-nd ra-fast-retrans** to enable or disable the IPv6 Router Advertisement fast retransmit feature. According to RFC4861, consecutive RA packets should be sent with at least 3 seconds delay. PICOS by default bypasses this restriction by fast transmission of RA to achieve better convergence.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd ra-fast-retrans <true|false>**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
ra-fast-retrans <true|false>	Enables or disables the Fast Retransmit feature. • **true:** Enables RA packet fast retransmit • **false:** Disables RA packet fast retransmit Default is enabled.

Example

- This example enables RA fast retransmit.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd ra-fast-retrans true
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd ra-interval

To set the RA interval, run the command **set l3-interface routed-interface ipv6-nd ra-interval**. This sets the time between unsolicited RA packets sent by the device on the specified interface. RA interval can be set in milliseconds or in seconds.

Run the command **delete l3-interface routed-interface ipv6-nd ra-interval** to remove this configuration and go back to the default interval of 60 seconds.

Command Syntax

set l3-interface routed-interface <*interface-name***> ipv6-nd ra-interval {sec <***seconds***> | msec <***milliseconds***>}**

delete l3-interface routed-interface <*interface-name***> ipv6-nd ra-interval {sec|msec}**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
sec <*seconds***>**	Specifies the interval in seconds, the value ranges from 1 to 1800 seconds. The default is 60 seconds.
msec <*milliseconds***>**	Specifies the interval in milliseconds, the value ranges from 70 to 1800000 milliseconds. The default value is 600000ms.

Example

- This example configures the RA interval to 50 seconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd ra-interval sec 50
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd ra-lifetime

Run the command **set l3-interface routed-interface ipv6-nd ra-lifetime** to configure the router lifetime field in the RA packets. This interval in seconds, indicate the effectiveness of the router on this link. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd ra-lifetime <***seconds*>

delete l3-interface routed-interface <*interface-name*> **ipv6-nd ra-lifetime**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
ra-lifetime <*seconds*>	Specifies the router lifetime interval in seconds. The value ranges from 0 to 9000. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Example

- This example configures an IPv6 router lifetime to 2000 seconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd ra-lifetime 2000
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd reachable-time

Run the command **set l3-interface routed-interface ipv6-nd reachable-time** to configure the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

The command **delete l3-interface routed-interface ipv6-nd reachable-time** sets the reachable time to the default value of 0. (no limit).

Command Syntax

set l3-interfacerouted-interface <*interface-name*> **ipv6-nd reachable-time <***reachable-time*>

delete l3-interface routed-interface <*interface-name*> **ipv6-nd reachable-time**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
reachable-time <*reachable-time*>	Specifies the reachable time in milliseconds. The value ranges from 1 to 3600000. The default value is 0, indicating no limit.

Example

- This example configures an IPv6 reachable time to 2000 milliseconds.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd reachable-time 2000
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd router-preference

Run the command **set l3-interface routed-interface ipv6-nd router-preference** to set the IPv6 Default Router Preference. Routers may include the default router preference in RA packets to signal to nodes the router preference in *low, medium* or *high.* Router preference is sent using the unused bits in the RA packet. The hosts that do not implement the default router preference will ignore these bits.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd router-preference <low|medium|high>**

delete l3-interface routed-interface <*interface-name*> **ipv6-nd router-preference**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
router-preference <low|medium|high>	Specifies the default router preference, the three possible values are *low, medium* and *high.* • **low:** Specifies a low default router preference. • **medium:** Specifies a medium default router preference. • **high :** Specifies a high default router preference. The default is medium default router preference.

Example

- The command below sets the default router preference to low.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd router-preference low
admin@XorPlus# commit
```

set l3-interface routed-interface ipv6-nd suppress-ra

Run the command **set l3-interface routed-interface ipv6-nd supress-ra** to enable or disable sending Router Advertisement (RA) on the specified routed interface or sub-interface.

Command Syntax

set l3-interface routed-interface <*interface-name*> **ipv6-nd suppress-ra true**

set l3-interface routed-interface <*interface-name*> **ipv6-nd suppress-ra false**

Parameters

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
true	Disables sending RA packets.
false	This option enables sending RA packets.

Example

- This example enables sending RA packets on routed interface *rif-te4*.

```
admin@XorPlus# set l3-interface routed-interface rif-te4 ipv6-nd suppress-ra false
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd adv-interval-option

Run the command **set l3-interface vlan-interface ipv6-nd adv-interval-option** to include the advertisement interval option in the RA packets. The Advertisement Interval Option indicates to host the maximum time in milliseconds between successive unsolicited Router Advertisements.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd adv-interval-option**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd adv-interval-option**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
adv-interval-option	Indicates the Ra packet advertisement interval option.

Example

- This example includes the advertisement interval option in RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd adv-interval-option
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd home-agent-config-flag

Run the command **set l3-interface vlan-interface ipv6-nd home-agent-config-flag** to set or unset the home agent config flag in RA packets. The Home Agent Option flag can be set or unset in IPv6 RA packets and is used to indicate to hosts that the router acts as Home Agent and includes a Home Agent Option. This option is not set by default.

Run the command **delete l3-interface vlan-interface vlan4001 ipv6-nd home-agent-config-flag** to unset the flag.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-config-flag**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-config-flag**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
home-agent-config-flag	Indicates the home agent config flag in the RA packet.

Example

- This example command sets the home agent config flag in the RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-config-flag
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd home-agent-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd home-agent-lifetime** to set the home agent lifetime value in seconds. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the current Router Lifetime value.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-lifetime <***seconds***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-lifetime <***seconds***>**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
home-agent-lifetime <*seconds*>	Specifies the home agent lifetime in seconds. The value is an integer that ranges from 0 to 65520. The default value is 0.

Example

- This example configures the home agent lifetime to 5 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-lifetime 5
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd home-agent-preference

Run the command **set l3-interface vlan-interface ipv6-nd home-agent-preference** to configure the home agent preference in RA packets. This parameter specifies the value to be placed in Home Agent Option when its set. The default value is 0 which means the least preferred.

Run the command **delete l3-interface vlan-interface ipv6-nd home-agent-preference** to delete this configuration and revert to the default value of 0.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-preference <***preference***>**

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd home-agent-preference <***preference***>**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
home-agent-preference <*preference***>**	Specifies the home agent preference. The value is an integer that ranges from 0 to 65535. The default value is 0.

Example

- This example configures the home agent preference to 5.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd home-agent-preference 5
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd managed-config-flag

Run the command **set l3-interface vlan-interface ipv6-nd managed-config-flag** to set or unset the managed config flag in the IPv6 RA packets. This flag indicates to the hosts that they must use managed protocol or stateful addresses autoconfiguration besides any addresses autoconfigured using stateless address autoconfiguration.

This flag is not set by default. To delete this configuration or unset the flag, run the command **delete l3-interface vlan-interface ipv6-nd managed-config-flag.**

Command Syntax

set l3-interface vlan-interface <*interface-name***> ipv6-nd managed-config-flag**

delete l3-interface vlan-interface <*interface-name***> ipv6-nd managed-config-flag**

Parameters

Parameter	Description
vlan-interface <*interface-name***>**	Specifies the VLAN interface name. The value is a string.

Example

- This example sets the managed config flag in the RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd managed-config-flag
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd mtu

Run the command **set l3-interface vlan-interface ipv6-nd mtu** to include the MTU option is RA packets. This option assists the hosts in proper interface configuration. The advertised MTU is not verified to be consistent with the actual router interface MTU.

Run the command **delete l3-interface vlan-interface ipv6-nd mtu** to delete this option. This value is not configured in RA packets by default.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd mtu <***value***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd mtu**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
mtu <*value***>**	Specifies the MTU value to advertise in RA packets. The value is an integer that ranges from 1 65535.

Example

- This example configures the advertised MTU value to 1000.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd mtu 1000
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd other-config-flag

Run the command **set l3-interface vlan-interface ipv6-nd other-config-flag** to set the *other config flag* in RA packets. This flag indicates to hosts that administered or stateful protocol should be used for autoconfiguration information other than addresses. This flag is not set by default.

Run the command **delete l3-interface vlan-interface ipv6-nd other-config-flag** to unset this flag in RA packets.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd other-config-flag**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd other-config-flag**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.

Example

- This example sets the *other config flat* in RA packets.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd other-config-flag
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix off-link

Run the command **set l3-interface vlan-interface ipv6-nd prefix** to configure an IPv6 prefix to include in RA packets without specifying on-link or off-link properties of the advertised prefix. The off-link option is not set by default which means the prefix can be used for on-link determination. The optional parameter **no-autoconfig** can be used to indicate to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix** <*IPv6 Prefix*> **off-link [no-autoconfig]**

delete l3-interface vlan-interface <*vlan-interface*> ipv6-nd prefix <*IPv6 Prefix***> off-link [no-autoconfig]**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
no-autoconfig	This option indicates to hosts on local link that the prefix cannot be used for IPv6 autoconfiguration.

Example

- This example configures an IPv6 prefix with off-link and no-autoconfig options.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 off-link no-autoconfig
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd prefix preferred-lifetime** to configure the advertised prefix preferred lifetime in seconds. Addresses generated from the prefix during this time period will be considered preferred addresses.

Run the command **delete l3-interface vlan-interface ipv6-nd prefix preferred-lifetime** to remove this configuration.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix prefix <***IPv6 Prefix***> preferred-lifetime <***seconds* **| infinite>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix prefix <***IPv6 Prefix***> preferred-lifetime**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
preferred-lifetime <*seconds* **| infinite>**	Specifies the time the addresses are treated as preferred addresses. The value could be in seconds from 0 to 4294967295 with default value of 604800 or use keyword **infinite** indicating infinity.

Example

- This example configures an IPv6 prefix with with infinite preferred lifetime.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 preferred-lifetime infinite
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix router-address

Run the command **set l3-interface vlan-interface ipv6-nd prefix router-address** to set the R flag to indicate to hosts on local link that the specified prefix contains a complete IP address. This flag is not set by default which means hosts do not assume a complete IP address is placed.

Run the command **delete l3-interface vlan-interface ipv6-nd prefix router-address** to unset this flag.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> router-address**

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> router-address**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64.

Example

- This example sets the R flag for the given prefix.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 router-address
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd prefix valid-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd prefix valid-lifetime** to configure the time in seconds during which the prefix is considered valid for on-link determination.

Run the command **delete l3-interface vlan-interface ipv6-nd prefix valid-lifetime** to delete this configuration and revert to the default value of 2592000 seconds.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> valid-lifetime <***seconds* **| infinite>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd prefix <***IPv6 Prefix***> valid-lifetime**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
prefix <*IPv6 Prefix*>	Specifies the IPv6 prefix, e.g. fa00::0/64
valid-lifetime <*seconds* **| infinite>**	Specifies the time period for which the prefix is valid. The value could be in seconds, Range: (0-4294967295) Default: 2592000. Or it could be **infinite** indicating infinite time.

Example

- This example configures the valid time of IPv6 prefix to infinity.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd prefix fa00::0/64 valid-lifetime infinite
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd ra-fast-retrans

Run the command **set l3-interface vlan-interface ipv6-nd ra-fast-retrans** to enable or disable the IPv6 Router Advertisement fast retransmit feature. According to RFC4861, consecutive RA packets should be sent with at least 3 seconds delay. PICOS by default bypasses this restriction by fast transmission of RA to achieve better convergence.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd ra-fast-retrans <true|false>**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
ra-fast-retrans <true|false>	Enables or disables the Fast Retransmit feature. • **true:** Enables RA packet fast retransmit • **false:** Disables RA packet fast retransmit Default is enabled.

Example

- This example enables RA fast retransmit.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-fast-retrans true
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd ra-interval

To set the RA interval, run the command **set l3-interface vlan-interface ipv6-nd ra-interval**. This sets the time between unsolicited RA packets sent by the device on the specified interface. RA interval can be set in milliseconds or in seconds.

Run the command **delete l3-interface vlan-interface ipv6-nd ra-interval** to remove this configuration and go back to the default interval of 60 seconds.

Command Syntax

set l3-interface vlan-interface <*interface-name***> ipv6-nd ra-interval {sec <***seconds***> | msec <***milliseconds***>}**

delete l3-interface vlan-interface <*interface-name***> ipv6-nd ra-interval {sec|msec}**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
sec <*seconds***>**	Specifies the interval in seconds, the value ranges from 1 to 1800 seconds. The default is 60 seconds.
msec <*milliseconds***>**	Specifies the interval in milliseconds, the value ranges from 70 to 1800000 milliseconds. The default value is 600000ms.

Example

- This example configures the RA interval to 50 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-interval sec 50
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd ra-lifetime

Run the command **set l3-interface vlan-interface ipv6-nd ra-lifetime** to configure the router lifetime field in the RA packets. This interval in seconds, indicate the effectiveness of the router on this link. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Command Syntax

set l3-interfacevlan-interface <*vlan-interface***> ipv6-nd ra-lifetime <***seconds***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd ra-lifetime**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
ra-lifetime <*seconds***>**	Specifies the router lifetime interval in seconds. The value ranges from 0 to 9000. If set to zero, means the hosts should not consider it as a default router on this interface. The value must be either zero or between a value configured with the IPv6 RA interval command (or default value) and 9000 seconds. The default value is 1800 seconds.

Example

- This example configures an IPv6 router lifetime to 2000 seconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd ra-lifetime 2000
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd reachable-time

Run the command **set l3-interface vlan-interface ipv6-nd reachable-time** to configure the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

The command **delete l3-interface vlan-interface ipv6-nd reachable-time** sets the reachable time to the default value of 0. (no limit).

Command Syntax

set l3-interfacevlan-interface <*vlan-interface***> ipv6-nd reachable-time <***reachable-time***>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd reachable-time**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
reachable-time <*reachable-time***>**	Specifies the reachable time in milliseconds. The value ranges from 1 to 3600000. The default value is 0, indicating no limit.

Example

- This example configures an IPv6 reachable time to 2000 milliseconds.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd reachable-time 2000
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd router-preference

Run the command **set l3-interface vlan-interface ipv6-nd router-preference** to set the IPv6 Default Router Preference. Routers may include the default router preference in RA packets to signal to nodes the router preference in *low, medium* or *high.* Router preference is sent using the unused bits in the RA packet. The hosts that do not implement the default router preference will ignore these bits.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd router-preference <low|medium|high>**

delete l3-interface vlan-interface <*vlan-interface***> ipv6-nd router-preference**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name.
router-preference <low|medium|high>	Specifies the default router preference, the three possible values are *low, medium* and *high.* • **low:** Specifies a low default router preference. • **medium:** Specifies a medium default router preference. • **high :** Specifies a high default router preference. The default is medium default router preference.

Example

- The command below sets the default router preference to low..

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd router-preference low
admin@XorPlus# commit
```

set l3-interface vlan-interface ipv6-nd suppress-ra

Run the command **set l3-interface vlan-interface ipv6-nd supress-ra** to enable or disable sending Router Advertisement (RA) on the specified VLAN interface.

Command Syntax

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd suppress-ra true**

set l3-interface vlan-interface <*vlan-interface***> ipv6-nd suppress-ra false**

Parameters

Parameter	Description
vlan-interface <*vlan-interface***>**	Specifies the VLAN interface name. The value is a string.
true	Disables sending RA packets.
false	This option enables sending RA packets.

Example

- This example enables sending RA packets on interface vlan200.

```
admin@XorPlus# set l3-interface vlan-interface vlan4001 ipv6-nd suppress-ra false
admin@XorPlus# commit
```

set management-ethernet-speed eth0

The **set management-ethernet-speed eth0** command configures port speed of **eth0** out-of-band management interface in operational mode.

Command Syntax

set management-ethernet-speed eth0 <**10 | 100 | 1000 | auto**>

Parameter

Null.

Example

- Configure port speed of **eth0** out-of-band management interface to 100Mbit/s and show the configuration result.

```
admin@PICOS> set management-ethernet-speed eth0 100
admin@PICOS> start shell sh
admin@PICOS:~$ sudo ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  Not reported
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: No
        Advertised FEC modes: Not reported
        Speed: 100Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 2
        Transceiver: internal
        Auto-negotiation: off
        MDI-X: Unknown
```

set interface gigabit-ethernet up-mode

This command makes a local MAC layer to keep up status. This command generally coordinates with another command of interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean> when RX link of fiber breaks. If the two commands are configured together, TX link can still transmit traffic.

> **Caution:**
> Do not configure up-mode with UDLD, as this may cause the peer interface to be disabled unexpectedly by UDLD.

Command Syntax

set interface gigabit-ethernet <*port*> **up-mode** <*boolean*>

Parameter

<*port*> Ethernet port, now only support 10GE, 40GE, 100GE port .

<*boolean*> vaule is false or true. Default value is false.

Example

This example shows how to configure this command:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 up-mode true
admin@XorPlus# commit
```

set interface gigabit-ethernet speed

The **set interface gigabit-ethernet speed** command sets the force rate of an interface or enable auto-negotiation mode.

Command Syntax

set interface gigabit-ethernet<*interface-name*> **speed** [**auto** | <*speed*>]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name***>**	Specifies the interface name.
speed [**auto** | <*speed*>]	Specifies the interface rate. The values can be **auto** or <*speed*>. • **auto**: Sets the Ethernet interface to work in auto-negotiation mode. See Configuring the Auto-Negotiation Mode for details. • <*speed*>: Specifies an interface rate. The unit is **Mbit/s**.

Usage Guidelines

Interface rate can be configured in the two modes: force rate (non-auto-negotiation mode) and auto-negotiation mode.

> **NOTE:**
>
> Interfaces at both ends of a link SHOULD work in the same auto-negotiation mode. Otherwise, the interfaces may not be able to communicate with each other.

Instructions for the switch interface rate configuration:

1. 1G RJ45 port: The interface rate can be configured to 100M, 10M or auto. By default, the interfaces work in auto-negotiation mode.
2. 1G optical port: The interface rate can be configured to 1000M or auto. By default, the interfaces work in auto-negotiation mode.
3. 10G RJ45 port: The interface rate can be configured to 100M or auto. By default, the interfaces work in auto-negotiation mode.
4. 10G optical port:
   - When a 10G optical module is inserted, the interface rate can be configured to 10G or 1G. When no force rate is configured, the interface recognizes the interface rate of itself as 10G.
   - When a 1G optical module is inserted, the interface rate can be configured to 1G. When no force rate is configured, the interface recognizes the interface rate of itself as 1G.
5. 40G optical port: The interface rate can be configured to 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 40G. If the interface configured interface split, the split interface rate can be configured to 10G or 1G.
6. 100G optical port:
   - When a 100G optical module is inserted, the interface rate can be configured to 100G or 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 100G. If the interface configured interface split, the split interface rate can be configured to 25G or 10G.
   - When a 40G optical module is inserted, the interface rate can be configured to 40G. When no force rate is configured, the interface recognizes the interface rate of itself as 40G. If the interface configured interface split, the split interface rate can be configured to 10G.
7. 400G optical port: The interface rate can be configured to 400G or 100G. When no force rate is configured, the interface recognizes the interface rate of itself as 400G. If the interface configured interface split, the split interface rate can be configured to 100G.

Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode. By default, these interfaces work in auto-negotiation mode. In auto-negotiation mode the ports negotiate any rate supported by the two devices. If the negotiated interface rate is not the required value, you can use the **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** command to manually specify the auto-negotiation rate to make the interface negotiate the rate within the specified range.

Example

- Configure the force rate of the Te-1/1/49 port to 100Mbit/s.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/49 speed 100
admin@XorPlus# commit
```

show interface bpdu-tunneling

This command is to show bpdu tunneling on all interface.

Command Syntax
run show interface bpdu-tunneling

Example
• This example is to show bpdu tunneling:

```
admin@XorPlus# run show interface bpdu-tunneling
Destination Mac: 1:e:0:0:0:1
```

show interface aggregate-ethernet <lag_name>

This command is to show information about the specified LAG interface.

Command Syntax
run show interface aggregate-ethernet <*lag_name*> *[text]*

Parameter
•<*lag_name*> Name of LAG interface.
• [*text*] The special information. Options include:

- **brief** Show brief information
- **detail** Show detail information

Example
• This example is to show information of ae1:

```
admin@XorPlus# run show interface aggregate-ethernet ae1
Physical interface: ae1, Enabled, error-discard False, Physical link is Down
Interface index: 53
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Current address: 08:9e:01:a8:00:49, Hardware address: 08:9e:01:a8:00:49
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 0 bits/sec, 0 packets/sec
Input Packets.............................0
Output Packets............................0
Input Octets..............................0
Output Octets............................0
Aggregated link protocol: STATIC
Minimum number of selected ports: 1
Members Status Port Speed
--------- ---------- ----------
```

show interface aggregate-ethernet <lag_name> dot1q-tunneling

This command is to show dot1q-tunneling on a specified LAG.

Command Syntax
run show interface aggregate-ethernet <*lag_name*> dot1q-tunneling

Parameter
•<*lag_name*> Name of LAG interface.

Example
• This example is to show bpdu tunneling:

```
admin@XorPlus# run show interface aggregate-ethernet ae1 dot1q-tunneling
Dot1q Tunneling Mode: internal, Ether Type: 0x8100
```

show interface brief

This command show interface brief information ,this information includes Interface name, Management,Status, Flow Control, Duplex ,Speed ,Description.

Command Syntax
run show interface brief

Example
• This example is to show brief information of interface.

```
admin@Xorplus#  run show interface brief
Interface       Management  Status  Flow Control  Duplex  Speed    Description
--------------  ----------  ------  ------------  ------  -------  ------------------------------
ge-1/1/1        Enabled     Down    Disabled      Full    Auto
ge-1/1/2        Enabled     Down    Disabled      Full    Auto
ge-1/1/3        Enabled     Down    Disabled      Full    Auto
ge-1/1/4        Enabled     Down    Disabled      Full    Auto
ge-1/1/5        Enabled     Down    Disabled      Full    Auto
ge-1/1/6        Enabled     Down    Disabled      Full    Auto
ge-1/1/7        Enabled     Down    Disabled      Full    Auto
ge-1/1/8        Enabled     Down    Disabled      Full    Auto
ge-1/1/9        Enabled     Down    Disabled      Full    Auto
ge-1/1/10       Enabled     Down    Disabled      Full    Auto
ge-1/1/11       Enabled     Down    Disabled      Full    Auto
ge-1/1/12       Enabled     Down    Disabled      Full    Auto
ge-1/1/13       Enabled     Down    Disabled      Full    Auto
ge-1/1/14       Enabled     Down    Disabled      Full    Auto
ge-1/1/15       Enabled     Down    Disabled      Full    Auto
ge-1/1/16       Enabled     Down    Disabled      Full    Auto
ge-1/1/17       Enabled     Down    Disabled      Full    Auto
ge-1/1/18       Enabled     Down    Disabled      Full    Auto
ge-1/1/19       Enabled     Down    Disabled      Full    Auto
ge-1/1/20       Enabled     Down    Disabled      Full    Auto
ge-1/1/21       Enabled     Down    Disabled      Full    Auto
ge-1/1/22       Enabled     Down    Disabled      Full    Auto
ge-1/1/23       Enabled     Down    Disabled      Full    Auto
ge-1/1/24       Enabled     Down    Disabled      Full    Auto
ge-1/1/25       Enabled     Down    Disabled      Full    Auto
ge-1/1/26       Enabled     Down    Disabled      Full    Auto
ge-1/1/27       Enabled     Down    Disabled      Full    Auto
ge-1/1/28       Enabled     Down    Disabled      Full    Auto
ge-1/1/29       Enabled     Down    Disabled      Full    Auto
ge-1/1/30       Enabled     Down    Disabled      Full    Auto
ge-1/1/31       Enabled     Up      Disabled      Full    1Gb/s
ge-1/1/32       Enabled     Up      Disabled      Full    1Gb/s
ge-1/1/33       Enabled     Down    Disabled      Full    Auto
ge-1/1/34       Enabled     Down    Disabled      Full    Auto
ge-1/1/35       Enabled     Down    Disabled      Full    Auto
ge-1/1/36       Enabled     Down    Disabled      Full    Auto
ge-1/1/37       Enabled     Down    Disabled      Full    Auto
ge-1/1/38       Enabled     Down    Disabled      Full    Auto
ge-1/1/39       Enabled     Down    Disabled      Full    Auto
ge-1/1/40       Enabled     Down    Disabled      Full    Auto
ge-1/1/41       Enabled     Down    Disabled      Full    Auto
ge-1/1/42       Enabled     Down    Disabled      Full    Auto
ge-1/1/43       Enabled     Down    Disabled      Full    Auto
ge-1/1/44       Enabled     Down    Disabled      Full    Auto
ge-1/1/45       Enabled     Down    Disabled      Full    Auto
ge-1/1/46       Enabled     Down    Disabled      Full    Auto
ge-1/1/47       Enabled     Down    Disabled      Full    Auto
ge-1/1/48       Enabled     Down    Disabled      Full    Auto
te-1/1/1(49)    Enabled     Up      Disabled      Full    10Gb/s
```

```
te-1/1/2(50)    Enabled     Down    Disabled      Full    10Gb/s
```

The number (49), (50) with the interface name are the physical port labels of the interface.

show interface detail

This command show interface detail information.

Command Syntax
run show interface detail

Example
• This example is to show detail information of interface :

```
admin@XorPlus# run show interface detail
Physical interface: ge-1/1/1, Enabled, error-discard False, Physical link is Up
Interface index: 1, SFP type: Unknown
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: 100Mb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit ingress:100, egress:100
Current address: 08:9e:01:a8:00:49, Hardware address: 08:9e:01:a8:00:49
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 392 bits/sec, 0 packets/sec
Input Packets.....................99114129
Output Packets.....................57388
Input Octets.....................6343304256
Output Octets.....................7021889
Transmit:
Unicast packets.....................0
Multicast packets.....................57388
Broadcast packets.....................0
Packets 64 Octets.....................0
Packets 65-127 Octets.................55264
Packets 128-255 Octets.................2124
Packets 256-511 Octets.................0
Packets 512-1023 Octets................0
Packets 1024-1518 Octets...............0
Oversize Packets.....................0
Total Packets Without Errors..........57388
Discarded Packets.....................0
Total Packets With Errors.............0
Single Collision Frames...............0
Multiple Collision Frames.............0
Deferred Frames.....................0
Late Collisions.....................0
Excessive Collisions..................0
Pause Frames.....................0
Receive:
Unicast packets.....................99114129
-More-
```

show interface diagnostics optics all

This command is to show diagnostics informations of all interface or a specified interface.

Command Syntax
run show interface diagnostics optics [**all** | *<interface-name>*]

Example
• This example is to show diagnostics informations:

```
admin@Xorplus# run show interface diagnostics optics all
Interface       Temp(C/F)    Voltage(V)  Bias(mA)  Tx Power(dBm)  Rx Power(dBm)  Module Type
--------------  -----------  ----------  --------  -------------  -------------  -----------
te-1/1/1(49)    27.78/82.00  3.27        6.88      -3.38          -20.00         10G_BASE_SR


admin@Xorplus# run show interface diagnostics optics te-1/1/1
Interface       Temp(C/F)    Voltage(V)  Bias(mA)  Tx Power(dBm)  Rx Power(dBm)  Module Type
--------------  -----------  ----------  --------  -------------  -------------  -----------
te-1/1/1(49)    27.78/82.00  3.27        6.88      -3.38          -20.00         10G_BASE_SR
```

The number (49) with the interface name is the physical port label of the interface.

show interface ecmp max-path

This command is to show max counter of ecmp path.

Example
• This example is to show max counter of ecmp path:

```
admin@XorPlus# run show interface ecmp max-path
max-path:   4
```

show interface flexlink

This command is to show flexlink information.

Command Syntax
run show interface flexlink

Example
• This example is to show flexlink on all interfaces:

```
admin@XorPlus# run show interface flexlink
Active Interface Backup Interface Mode Delay(seconds)
---------------- ---------------- --------- --------------
ge-1/1/1(up) ge-1/1/2(standby) off 0
```

show interface gigabit-ethernet <interface>

This command is to show brief,detail or dot1q-tunneling information of a specified port.

Command Syntax
run show interface gigabit-ethernet *<interface> [text]*

Parameter
•*<interfce>* a specified interface identifier,[ge-1/1/1...ge-1/1/48],[te-1/1/49...te-1/1/52]
•*[text]* The special information.

- **brief** Show interface brief information
- **detail** Show interface detail information
- **dot1q-tunneling** Show dot1q tunneling information about the specified interface

Example
• This example is to show detail information on ge-1/1/3:

```
admin@XorPlus# run show interface gigabit-ethernet ge-1/1/3 detail
Physical interface: ge-1/1/3, Enabled, error-discard False, Physical link is Up
Interface index: 3, SFP type: Unknown, Mac Learning Enabled
Port mode: access
Description:
Link-level type: Ethernet, MTU: 1514, Speed: 100Mb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Interface rate limit ingress:0, egress:0
Current address: 08:9e:01:a8:00:49, Hardware address: 08:9e:01:a8:00:49
Traffic statistics:
5 sec input rate 0 bits/sec, 0 packets/sec
5 sec output rate 392 bits/sec, 0 packets/sec
Input Packets.............................10000
Output Packets............................186601
Input Octets..............................640000
Output Octets............................15763131
Transmit:
Unicast packets.......................91800
Multicast packets.....................64781
Broadcast packets.....................30020
Packets 64 Octets.....................121822
Packets 65-127 Octets.................64777
Packets 128-255 Octets.................2
Packets 256-511 Octets.................0
Packets 512-1023 Octets................0
Packets 1024-1518 Octets...............0
Oversize Packets.......................0
Total Packets Without Errors...........186601
Discarded Packets......................0
Total Packets With Errors..............0
Single Collision Frames................0
Multiple Collision Frames..............0
Deferred Frames........................0
Late Collisions........................0
Excessive Collisions...................0
Pause Frames...........................0
Receive:
Unicast packets.......................10000
Multicast packets.....................0
Broadcast packets.....................0
Packets 64 Octets.....................10000
Packets 65-127 Octets.................0
Packets 128-255 Octets.................0
Packets 256-511 Octets.................0
```

```
Packets 512-1023 Octets.............0
Packets 1024-1518 Octets............0
Oversize Packets....................0
Total Packets Without Errors..........10000
Discarded Packets...................0
Total Packets With Errors.............0
Alignment Errors....................0
FCS Errors..........................0
Collisions..........................0
Pause Frames........................0



admin@Xorplus# run show interface gigabit-ethernet te-1/1/1
Physical interface: te-1/1/1(49), Enabled, error-discard False, Physical link is Up
Interface index: 49, SFP+ type: 10G_BASE_SR, Mac Learning Enabled
Description:
Link-level type: Ethernet, MTU: 1518, Speed: 10Gb/s, Duplex: Full
Source filtering: Disabled, Flow control: Disabled
Auto-negotiation: Disabled
Interface flags: SNMP-Traps Internal: 0x0
Interface rate limit  ingress:unlimited, egress:unlimited
Interface burst limit ingress:unlimited, egress:unlimited
Link fault signaling  ignore local fault:false, ignore remote fault:false
force up mode:true
Precision Time Protocol mode:none
Current address: 1c:72:1d:c9:1b:e1, Hardware address: 1c:72:1d:c9:1b:e1
Traffic statistics:
  5 sec input rate 0 bits/sec, 0 packets/sec
  5 sec output rate 1607765248 bits/sec, 2450861 packets/sec
  Input Packets.....................0
  Output Packets....................17156180968
  Input Octets......................0
  Output Octets.....................1406807017424
```

set interface gigabit-ethernet fec

The **set interface gigabit-ethernet fec** command is used to enable or disable Forwarding Error Correction (FEC) function on the 100G, 40G or 25G port of the switch.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **fec** <**true | false**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the 100G, 40G or 25G interface name of the switch.
fec <**true	false**>	Enable or disable FEC function. The value could be **true** or **false**. • **true**: enables FEC function. • **false**: disables FEC function. By default, FEC function is disabled.

Example

- Disable FEC function on the switch port xe-1/1/1.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/1 fec false
admin@XorPlus# commit
```

- Enable FEC function on the switch port xe-1/1/2.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/2 fec true
admin@XorPlus# commit
```

set interface gigabit-ethernet family ethernet-switching vlan members

This command is to add a vlan member to this trunk port with tagged packet, vlan members range from 1 to 4094. The default of this command is that packets are tagged when the packets go out from this interface.

Note: If this interface's native-vlan-id is identical to vlan-member, packets will be encapsulated with vlan tag because tagged packet is the default configuration of vlan-member.

Command Syntax
set interface gigabit-ethernet *<port>* **family ethernet-switching vlan members** *<vlan-id>*
delete interface gigabit-ethernet *<port>* **family ethernet-switching vlan members** *<vlan-id>*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.

• *<vlan-id>* Configure the VLAN ID or VLAN ID range for which the interface can carry traffic, eg: 2, 3... Range: 1 to 4094.

> **NOTE:**
> When configuring VLAN member, use VLAN ID or VLAN range, but NOT other strings.

Example

• This example is adding a trunk port (ge-1/1/3) to a VLAN:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 5
admin@XorPlus# commit
```

• This example is adding a trunk port (ge-1/1/30) to a VLAN range:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/30 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/30 family ethernet-switching vlan members 50-100
admin@XorPlus# commit
```

• This example is adding a trunk port (te-1/1/30) to VLAN 2 and 3:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/30 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet te-1/1/30 family ethernet-switching vlan members 2,3
admin@XorPlus# commit
```

set interface gigabit-ethernet family ethernet-switching port-mode

The **set interface gigabit-ethernet family ethernet-switching port-mode** command configures the port mode of a switch port.

Command Syntax

set interface gigabit-ethernet <*interface-name*> f**amily ethernet-switching port-mode** <*port-mode*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies a physical port name. The value is like ge-1/1/1, te-1/1/3.
port-mode <*port-mode*>	Specifies the port mode. The value could be **access**, **trunk**, **pvlan-host**, **pvlan-secondary-trunk**, **pvlan-promiscuous** or **pvlan-promiscuous-trunk**. • **access**: Configures the port mode to access. • **trunk**: Configures the port mode to trunk. • **pvlan-host**: Configures the port mode to pvlan-host. • **pvlan-secondary-trunk**: Configures the port mode to pvlan-secondary-trunk. • **pvlan-promiscuous**: Configures the port mode to pvlan-promiscuous. • **pvlan-promiscuous-trunk**: Configures the port mode to pvlan-promiscuous-trunk. By default, the port mode is access.

Usage Guidelines

There are six port modes, the last four of these modes are used for PVLAN. Only when configured with a PVLAN port mode, a port can be added into a private VLAN.

> **NOTE:**
>
> After modifying the port mode, the port will be restarted automatically.

The characteristics of different port modes:

- Access Port

An access interface connects to a user device. It can connect only to an access link, and Ethernet frames transmitted on the access link are untagged. An access interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the native VLAN ID.

- Trunk Port

A trunk interface connects to a switch and can connect only to a trunk link. A trunk interface allows frames from multiple VLANs to pass.

- PVLAN Host Port

A PVLAN host port connects to a user device. For host mode ports, make sure that their native VLAN is a secondary VLAN, otherwise the ports won't be able to forward packets from primary VLAN. One host port can be added into only one secondary VLAN.

Packets sent from this port are untagged.

- PVLAN Secondary Trunk Port

A PVLAN secondary trunk port is used to connect to the downstream devices. One secondary trunk port can be added into more than one secondary VLAN. Secondary trunk mode is applicable to scenarios where multiple secondary VLANs need to pass through the downlink port while Host mode is applicable to cases where only one secondary VLAN passes through the downlink port.

The primary VLAN ID carried by the packets is replaced with the corresponding secondary VLAN ID on the outbound side of the secondary trunk mode port, thus masking the primary VLAN for the downstream device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

> **NOTE:**
>
> - Secondary trunk mode ports can be added to only one secondary VLAN of the same primary VLAN, but can be added to multiple secondary VLANs associated with different primary VLANs.
> - PVLAN secondary trunk port can also be added to normal VLANs in addition to the secondary VLANs.

- PVLAN Promiscuous Port

PVLAN promiscuous ports are used to connect to the uplink devices. Uplinks are typically ports that connect to routers, firewalls, servers or provider networks.

Promiscuous ports belong to the primary VLAN, which can communicate with all PVLAN ports, including host/secondary trunk ports and other promiscuous/promiscuous trunk ports within the same primary VLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs.

Make sure that the native VLAN of the promiscuous port is the primary VLAN, otherwise the port will not forward packets sent from a secondary VLAN.

Promiscuous port mode is used when there is only one primary VLAN passing through the uplink port. Packets sent from this port are untagged.

- PVLAN Promiscuous Trunk Port

PVLAN promiscuous trunk ports are used to connect to the uplink devices. Promiscuous trunk port mode is used when there are more than one primary VLAN passing through the uplink port.

The secondary VLAN ID carried by the message is replaced with the corresponding primary VLAN ID on the outbound side of the port, thus masking the secondary VLAN for the uplink device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

> **NOTE:**
>
> PVLAN Promiscuous trunk ports can also be added to normal VLANs in addition to the primary VLANs.

Example

- Configure the port mode of ge-1/1/1 to access.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode access
admin@Xorplus# commit
```

set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol

The **set interface gigabit-ethernet family ethernet-switching bpdu-tunneling protocol** command enables the BPDU tunneling function of the Layer 2 protocol.

Command Syntax

set interface gigabit-ethernet <*port-id*> **family ethernet-switching bpdu-tunneling protocol** <*protocol-type*>

Parameter

Parameter	Description
gigabit-ethernet <*port-id*>	Specifies switch port identifier. Note: BPDU Tunneling cannot be configured on a LAG port, or the physical port that belongs to a LAG. When you need to configure BPDU tunneling on the physical port that belongs to a LAG, you need to first take the physical port out of the LAG port before configuration.
protocol <*protocol-type*>	Specifies the Layer 2 protocol, which needs to be transmitted through BPDU tunnel. The values could be **STP** or **LACP**.

Example

• Enable the BPDU tunneling function of STP protocol.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching bpdu-tunneling protocol stp
admin@XorPlus# commit
```

set interface gigabit-ethernet ether-options 802.3ad

The **set interface gigabit-ethernet ether-options 802.3ad** command adds a specified port to a LAG.

Command Syntax
set interface gigabit-ethernet <*interface-name***> ether-options 802.3ad** <*lag-interface-name*>
delete interface gigabit-ethernet <*interface-name***> ether-options 802.3ad**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name***>**	Specifies the ethernet switching port identifier which will be added to the LAG interface.
<*lag-interface-name*>	Specifies the name of the LAG interface. The value is a string in the format of **ae***x*. **Note**: The maximum LAGs per switch is limited by the interface capacity.

NOTE:

The maximum number of member ports per LAG is platform dependent, for details see Collection of Feature Specification of Different Platforms.

Example
• This example is to add ge-1/1/3 to ae1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 ether-options 802.3ad ae1
admin@XorPlus#commit
```

set interface gigabit-ethernet duplex auto

The **set interface gigabit-ethernet duplex auto** command configures the duplex mode of optical port as auto negotiation mode.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **duplex auto**

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the optical port name.

Usage Guidelines

Pay attention to the following notes:

- Currently, duplex mode for optical port is only available for the 10 optical port when its port rate set to 1G.
- Duplex mode for optical port currently only supports to configure as auto, i.e. auto negotiation mode.
- It is required that the duplex mode of the peer 1G optical port is also set to auto negotiation mode, otherwise the port cannot link up.

Use command **delete interface gigabit-ethernet** <*interface-name*> **duplex** to go back to the default duplex mode to full.

Example

- Set the duplex mode of optical port te-1/1/1 as auto negotiation mode.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 speed 1000
admin@Xorplus# set interface gigabit-ethernet te-1/1/1 duplex auto
```

set interface gigabit-ethernet cdr

The **set interface gigabit-ethernet cdr** command configures whether to enable or disable the CDR function.

> **NOTE:**
> - CDR function can only be configured on the 100G or 40G optical module interface and the four interfaces it breaked out from.
> - The CDR configurations of the four interfaces which breaked out from the 100G or 40G optical module interface should be the same.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **cdr** [**true | false**]

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical interface or split interface name. For example, te-1/1/49 and xe-1/1/49.1.
cdr [**true	false**]	Configures whether to enable or disable the CDR function. The value is **true** or **false**. **true**: enables the CDR function. **false**: disables the CDR function. The default value is **true**.

Example

- Enable the CDR function on interface te-1/1/49.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/49 cdr true
admin@Xorplus# commit
```

- Disable the CDR function on interface te-1/1/49.

```
admin@Xorplus# set interface gigabit-ethernet te-1/1/49 cdr false
admin@Xorplus# commit
```

set interface gigabit-ethernet breakout

The **set interface gigabit-ethernet breakout** command breaks out the 40G and 100G ports into four interfaces.

NOTE:

- Restart PICOS after commit this command to make the setting take effect.
- When performing the port breakout and merge operation, before restarting the system, you need to manually delete the configurations of the unavailable interfaces, to make sure that the configuration file can be loaded normally when the system boots up.
- From PICOS 3.7.3.4, AS7726_32X supports splitting a 100G port into 2x50G or 4x25G or 4x10G ports using command **set interface gigabit-ethernet** <*port-name*> **breakout true** and **set interface gigabit-ethernet breakmap** under L2/L3 mode.

Command Syntax

set interface gigabit-ethernet <*port-name*> **breakout** <**true | false**>

Parameter

Parameter	Description
gigabit-ethernet <*port-name*>	Specifies the port name of 40G or 100G port.
breakout <true | false>	Specifies the breakout mode. The value could be **true** or **false**. • **true**: Breakout the 40G or 100G port. • **false**: Not breakout the 40G or 100G port.

Usage Guidelines

The 40GE interfaces can be split into 4 x 10GE interfaces, the 100GE interface can be split into 4 x 25G or 4 x 10G Ethernet interfaces. By default, the 100G interface is split into 4 x 25G Ethernet interfaces. If you want to split into 4 x 10G Ethernet interfaces, you need to configure the four interfaces rate to 10G through the command line after port breakout. Note: The rate of the four interfaces is required to be consistent.

After a single interface is split into four interfaces, the 10GE split optical interface or the 25GE split optical interface supports the same configurations and features as other non-breakout optical interface except that the interface is named in a different way. For example, the port name of the 100GE and 40GE optical interfaces is xe-1/1/n before port breakout; however, after port breakout the port names of the four interfaces are xe-1/1/n.1, xe-1/1/n.2, xe-1/1 /n.3 and xe- 1/1/n.4.

Example

- Split the 40GE port xe-1/1/25 into 4 x 10GE ports.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/25 breakout true
admin@XorPlus# co
Commit OK.
Save done.
Interface breakout setting has been changed, please reboot the system for changes to take effect!
Make sure to delete all the configurations associated with the unavailable interfaces, otherwise loading startup co
admin@XorPlus# exit
admin@XorPlus> request system reboot
```

- Do not split the 100G port xe-1/1/53.

```
admin@XorPlus# set interface gigabit-ethernet xe-1/1/53 breakout false
admin@XorPlus# co
Commit OK.
Save done.
Interface breakout setting has been changed, please reboot the system for changes to take effect!
Make sure to delete all the configurations associated with the unavailable interfaces, otherwise loading startup co
admin@XorPlus# exit
admin@XorPlus> request system reboot
```

set interface gigabit-ethernet auto-speeds

The **set interface gigabit-ethernet auto-speeds** command sets the auto-negotiation rate of an interface in auto-negotiation mode.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **auto-speeds** <*auto-speed*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>**>**	Specifies the interface name.
auto-speeds <*auto-speed*>**>**	Specifies the auto-negotiation rate, the unit is **Mbit/s**. • For 1G RJ45port, the values of auto-negotiation rate could be 1000M, 100M or 10M. • For 10G RJ45 port, the values of auto-negotiation rate could be 10000M, 1000M or 100M. • For 5G/2.5G RJ45 port, the values of auto-negotiation rate could be 100M, 1000M, 2500M, 5000M and 10000M.

Usage Guidelines

NOTE:

- Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode and auto-negotiation rate.
- The auto-negotiation rates configured on the interfaces must have an intersection at both ends of the link.

Run the **set interface gigabit-ethernet**<*interface-name*> **speed auto** command to configure the Ethernet interface to work in auto-negotiation mode before using the **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** command to manually specify the auto-negotiation rate.

Only the 10G, 5G/2.5G and 1G RJ45 ports support auto-negotiation mode. By default, these interfaces work in auto-negotiation mode. In auto-negotiation mode the ports negotiate any rate supported by the two devices. If the negotiated interface rate is not the required value, you can use the **set interface gigabit-ethernet** <*interface-name*> **auto-speeds** command to manually specify the auto-negotiation rate to make the interface negotiate the rate within the specified range.

Example

- Set the auto-negotiation rates of ge-1/1/1 interface to 100M and 10M.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 100
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 10
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 speed auto
```

- Set the auto-negotiation rates of ge-1/1/1 interface to 1000M.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 auto-speeds 1000
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 speed auto
```

set interface ecmp hash-mapping field vlan disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." User can also enable additional fields like vlan.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field vlan disable <*bool*>
delete interface ecmp hash-mapping field vlan disable

Parameter
•<*bool*> disable including the field

- **true** disable vlan
- **false** enable vlan. Default.

Example
• This example is to enable vlan:

```
admin@XorPlus# set interface ecmp hash-mapping field vlan disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field port-source disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." User can also enable additional fields like port-source.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field port-source disable <*bool*>
delete interface ecmp hash-mapping field port-source disable

Parameter
•<*bool*> disable including the field

- **true** disable port-source
- **false** enable port-source. Default.

Example
• This example is to enable port-source:

```
admin@XorPlus# set interface ecmp hash-mapping field port-source disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field port-destination disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like port-destination.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field port-destination disable <*bool*>
delete interface ecmp hash-mapping field port-destination disable

Parameter
•<*bool*> disable including the field

- **true** disable port-destination
- **false** enable port-destination. Default.

Example
• This example is to enable port-destination:

```
admin@XorPlus# set interface ecmp hash-mapping field port-destination disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ip-source disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ip-source.

NOTE:
EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:

set interface ecmp hash-mapping field ingress-interface disable
set interface ecmp hash-mapping field ip-destination disable
set interface ecmp hash-mapping field ip-protocol disable
set interface ecmp hash-mapping field ip-source disable
set interface ecmp hash-mapping field port-destination disable
set interface ecmp hash-mapping field port-source disable
set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ip-source disable <*bool*>
delete interface ecmp hash-mapping field ip-source disable

Parameter
•<*bool*> disable including the field

- **true** disable ip-source
- **false** enable ip-source. Default.

Example
• This example is to enable ip-source:

```
admin@XorPlus# set interface ecmp hash-mapping field ip-source disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ip-protocol disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ip-protocol.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ip-protocol disable <*bool*>
delete interface ecmp hash-mapping field ip-protocol disable

Parameter
•<*bool*> disable including the field

- **true** disable ip-protocol
- **false** enable ip-protocol. Default.

Example
• This example is to enable ip-protocol:

```
admin@XorPlus# set interface ecmp hash-mapping field ip-protocol disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ip-destination disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ip-destination.

> **NOTE:**
> EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:
>
> set interface ecmp hash-mapping field ingress-interface disable
> set interface ecmp hash-mapping field ip-destination disable
> set interface ecmp hash-mapping field ip-protocol disable
> set interface ecmp hash-mapping field ip-source disable
> set interface ecmp hash-mapping field port-destination disable
> set interface ecmp hash-mapping field port-source disable
> set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ip-destination disable <*bool*>
delete interface ecmp hash-mapping field ip-destination disable

Parameter
•<*bool*> disable including the field

- **true** disable ip-destination
- **false** enable ip-destination. Default.

Example
• This example is to enable ip-destination:

```
admin@XorPlus# set interface ecmp hash-mapping field ip-destination disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping field ingress-interface disable

In the default setting, all fields are hashed by"ip-source," "port-destination," "port-source," and "vlan." Users can also enable additional fields like ingress-interface.

NOTE:
EVPN multihoming aliasing function uses the ECMP hash fields "ingress-interface","ip-destination", "ip-source," "port-destination," "port-source," and "vlan" for equivalent paths calculation. By default, all these fields are enabled. Users can run the following CLI commands to enable or disable the ECMP hash fields:

set interface ecmp hash-mapping field ingress-interface disable
set interface ecmp hash-mapping field ip-destination disable
set interface ecmp hash-mapping field ip-protocol disable
set interface ecmp hash-mapping field ip-source disable
set interface ecmp hash-mapping field port-destination disable
set interface ecmp hash-mapping field port-source disable
set interface ecmp hash-mapping field vlan disable

Command Syntax
set interface ecmp hash-mapping field ingress-interface disable <*bool*>
delete interface ecmp hash-mapping field ingress-interface disable

Parameter
•<*bool*> disable including the field

- **true** disable ingress-interface
- **false** enable ingress-interface. This is the default value.

Example
• This example is to enable ingress interface:

```
admin@XorPlus# set interface ecmp hash-mapping field ingress-interface disable false
admin@XorPlus# commit
```

set interface bpdu-tunneling destination-mac

The **set interface bpdu-tunneling destination-mac** command configures the BPDU tunneling destination multicast MAC address to replace the original destination multicast MAC address.

Command Syntax

set interface bpdu-tunneling destination-mac *<destination-mac>*

Parameter

Parameter	Description
destination-mac *<destination-mac>*	Specifies the destination multicast MAC address that replaces the destination multicast MAC address of Layer 2 protocol packets. The value is in H:H:H:H:H:H format. An H contains 2 hexadecimal numbers. The value ranges from 01:00:00:00:00:00 to 01:ff:ff:ff:ff:ff. The following multicast MAC addresses can not be used: 01:80:C2:00:00:00 to 01:80:C2:00:00:2f.

Example

• Configures the BPDU tunneling destination multicast MAC address to replace the original destination multicast MAC address.

```
admin@XorPlus# set interface bpdu-tunneling destination-mac 01:90:00:00:00:1a
admin@XorPlus# commit
```

set interface aggregate-ethernet family ethernet-switching vlan members

This command is to add a vlan member to the trunk lag, vlan members range from 1 to 4094. The default of this command is that packets are tagged when the packets go out from this interface.

Note: If this interface's native-vlan-id is identical to vlan-member, packets will be encapsulated with vlan tag because the " tagged" is the default configuration of vlan-member.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **family ethernet-switching vlan members** <*vlan-id*>
delete interface aggregate-ethernet <*lag_name*> **family ethernet-switching vlan members** <*vlan-id*>

Parameter
• <*lag_name*> Name of a LAG interface.
• <*vlan-id*> Configure the VLAN ID or VLAN ID range for which the interface can carry traffic, eg: 2, 3... Range: 1 to 4094.

> **NOTE:**
> When configuring VLAN member, use VLAN ID or VLAN range, but NOT other strings.

Example

• This example is adding a trunk LAG port (ae1) to a VLAN:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 5
admin@XorPlus# commit
```

• This example is adding a trunk LAG port (ae1) to a VLAN range:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 50-100
admin@XorPlus# commit
```

• This example is adding a trunk LAG port (ae1) to VLAN 2 and 3:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching vlan members 2,3
admin@XorPlus# commit
```

set interface aggregate-ethernet family ethernet-switching port-mode

The **set interface aggregate-ethernet family ethernet-switching port-mode** command configures the port mode of a switch LAG interface.

Command Syntax
set interface aggregate-ethernet <*lag-interface-name*> **family ethernet-switching port-mode** <*port-mode*>
delete interface aggregate-ethernet <*lag-interface-name*> **family ethernet-switching port-mode**

Parameter

Parameter	Description
aggregate-ethernet <*lag-interface-name*>	Specifies a LAG interface name. The value is like ae1, ae2.
port-mode <*port-mode*>	Specifies the port mode. The value could be **access**, **trunk**, **pvlan-host**, **pvlan-secondary-trunk**, **pvlan-promiscuous** or **pvlan-promiscuous-trunk**. • **access**: Configures the port mode as access. • **trunk**: Configures the port mode as trunk. • **pvlan-host**: Configures the port mode as pvlan-host. • **pvlan-secondary-trunk**: Configures the port mode as pvlan-secondary-trunk. • **pvlan-promiscuous**: Configures the port mode as pvlan-promiscuous. • **pvlan-promiscuous-trunk**: Configures the port mode to pvlan-promiscuous-trunk. By default, the port mode is access.

Usage Guidelines

There are six port modes, the last four of these modes are used for PVLAN. Only when configured with a PVLAN port mode, a port can be added into a private VLAN.

NOTE:

After modifying the port mode, the port will be restarted automatically.

The characteristics of different port modes:

- **Access Port**

An access interface connects to a user device. It can connect only to an access link, and Ethernet frames transmitted on the access link are untagged. An access interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the native VLAN ID.

- **Trunk Port**

A trunk interface connects to a switch and can connect only to a trunk link. A trunk interface allows frames from multiple VLANs to pass.

- **PVLAN Host Port**

A PVLAN host port connects to a user device. For host mode ports, make sure that their native VLAN is a secondary VLAN, otherwise the ports won't be able to forward packets from primary VLAN. One host port can be added into only one secondary VLAN.

Packets sent from this port are untagged.

- **PVLAN Secondary Trunk Port**

A PVLAN secondary trunk port is used to connect to the downstream devices. One secondary trunk port can be added into more than one secondary VLAN. Secondary trunk mode is applicable to scenarios where multiple secondary VLANs need to pass through the downlink port while Host mode is applicable to cases where only one secondary VLAN passes through the downlink port.

The primary VLAN ID carried by the packets is replaced with the corresponding secondary VLAN ID on the outbound side of the secondary trunk mode port, thus masking the primary VLAN for the downstream device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

NOTE:

- Secondary trunk mode ports can be added to only one secondary VLAN of the same primary VLAN, but can be added to multiple secondary VLANs associated with different primary VLANs.
- PVLAN secondary trunk port can also be added to normal VLANs in addition to the secondary VLANs.

- **PVLAN Promiscuous Port**

PVLAN promiscuous ports are used to connect to the uplink devices. Uplinks are typically ports that connect to routers, firewalls, servers or provider networks.

Promiscuous ports belong to the primary VLAN, which can communicate with all PVLAN ports, including host/secondary trunk ports and other promiscuous/promiscuous trunk ports within the same primary VLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs.

Make sure that the native VLAN of the promiscuous port is the primary VLAN, otherwise the port will not forward packets sent from a secondary VLAN.

Promiscuous port mode is used when there is only one primary VLAN passing through the uplink port. Packets sent from this port are untagged.

- **PVLAN Promiscuous Trunk Port**

PVLAN promiscuous trunk ports are used to connect to the uplink devices. Promiscuous trunk port mode is used when there are more than one primary VLAN passing through the uplink port.

The secondary VLAN ID carried by the message is replaced with the corresponding primary VLAN ID on the outbound side of the port, thus masking the secondary VLAN for the uplink device. By default, packets sent from this port will be tagged (tagged/untagged can be configured through CLI command).

> **NOTE:**
>
> PVLAN Promiscuous trunk ports can also be added to normal VLANs in addition to the primary VLANs.

Example
• This example sets ae1 port mode to trunk:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching port-mode trunk
admin@XorPlus# commit
```

set interface aggregate-ethernet disable

Enable or disable a LAG interface.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **disable** <true | false>

To delete the configuration enter:

delete interfaceaggregate-ethernet <*lag_name*> **disable**

Parameter

- <*lag_name*> Name of a LAG interface.
- true: disable a logical interface
- false: enable a logical interface

Example

This example disables the ae1 interface:

```
admin@XorPlus# set interface aggregate-ethernet ae1 disable true
admin@XorPlus# commit
```

set interface aggregate-ethernet description

Use this command to add a description to a LAG port.

Command Syntax
set interface aggregate-ethernett <*lag_name*> **description** <*description*>

To delete the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **description**

Parameter
• <*lag_name*> Name of LAG interface.
• <*description*> Add a human-readable description of the interface

Example
This example adds the description *hello* to port named ae1.

```
admin@XorPlus# set interface aggregate-ethernet ae1 description hello
admin@XorPlus# commit
```

set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout

The **set interface aggregate-ethernet aggregated-ether-options lacp fallback timeout** command configures the LACP fallback timer.

Command Syntax

set interface aggregate-ethernet <*lag-interface*> **aggregated-ether-options lacp fallback timeout** <*timer*>

Parameters

Parameter	Description
aggregate-ethernet <*lag-interface*>	Specifies the LAG interface name. The value is a string like ae1, ae99 and so on. NOTE: LACP fallback can only be applied on the LACP LAG interface, but not on a static LAG.
timeout <*timer*>	Specifies the timer to bring up a LAG and keeps one member port active. The value is an integer. The default value is 10 seconds.

Example

- Configure LACP fallback timer to 20 seconds.

```
admin@Xorplus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp fallback timeout 20
```

set interface aggregate-ethernet aggregated-ether-options lacp fallback enable

The **set interface aggregate-ethernet aggregated-ether-options lacp fallback enable** command can be used to enable or disable LACP fallback mode on a LAG interface.

Command Syntax

set interface aggregate-ethernet <*lag-interface*> **aggregated-ether-options lacp fallback enable** <**true | false**>

Parameters

Parameter	Description
aggregate-ethernet <*lag-interface*>	Specifies the LAG interface name. The value is a string like ae1, ae99 and so on. **NOTE:** LACP fallback can only be applied on the LACP LAG interface, but not on a static LAG.
enable <**true	false**>	Enable or disable LACP fallback feature. • **true**: Enable LACP fallback feature. • **false**: Disable LACP fallback feature.

Example

- Enable LACP fallback feature on LAG interface ae1.

```
admin@Xorplus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp fallback enable true
```

set interface aggregate-ethernet aggregated-ether-options lacp

Creates a Link Aggregation Control Protocol (LACP) link aggregation group (LAG) on a specified LAG port.

Command Syntax

set interface aggregate-ethernet <*lag_name*> **aggregated-ether-options lacp enable** <true | false>

To return the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **aggregated-ether-options lacp**

Parameter

- <*lag_name*> Enter the name of the LAG.
- true: enable LACP
- false: disable LACP

Example

This example configures LACP for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
admin@XorPlus# commit
```

set interface aggregate-ethernet

Use this command to create a Link Aggregation Group (LAG) interface.

Command Syntax

set interface aggregate-ethernet *<lag_name>*

Parameter

<lag_name> Enter the name of the LAG interface.

NOTE:

Before PicOS 2.9.2, the maximum number of LAGs is 48 on all models, that is, PicOS supports to configure LAG as ae1 to ae48 on all models.

In PicOS 2.9.2 and the later versions, the maximum number of LAGs is equal to the maximum number of physical interfaces by each model from ae1.

The maximum number of LAGs varies by platform, for details see Collection of Feature Specification of Different Platforms.

Example

The example creates a LAG named **ae4**.

```
admin@XorPlus# set interface aggregate-ethernet ae4
admin@XorPlus# commit
```

run show interface port-index-mapping

The **run show interface port-index-mapping** command shows the mapping informations between Logical Port Index and Physical Port Label.

Command Syntax
run show interface port-index-mapping

Example
• This example shows the interface mapping informations between the Logical Port Index and Physical Port Label.

Column "**Logical Port Index**" is logical interface name, "**Physical Port Label**" is same as the panel number of the physical port.

```
admin@Xorplus# run show interface port-index-mapping
Logical Port Index  Physical Port Label
------------------  -------------------
ge-1/1/1            1
ge-1/1/2            2
ge-1/1/3            3
ge-1/1/4            4
ge-1/1/5            5
ge-1/1/6            6
ge-1/1/7            7
ge-1/1/8            8
ge-1/1/9            9
ge-1/1/10           10
ge-1/1/11           11
ge-1/1/12           12
ge-1/1/13           13
ge-1/1/14           14
ge-1/1/15           15
ge-1/1/16           16
ge-1/1/17           17
ge-1/1/18           18
ge-1/1/19           19
ge-1/1/20           20
ge-1/1/21           21
ge-1/1/22           22
ge-1/1/23           23
ge-1/1/24           24
ge-1/1/25           25
ge-1/1/26           26
ge-1/1/27           27
ge-1/1/28           28
ge-1/1/29           29
ge-1/1/30           30
ge-1/1/31           31
ge-1/1/32           32
ge-1/1/33           33
ge-1/1/34           34
ge-1/1/35           35
ge-1/1/36           36
ge-1/1/37           37
ge-1/1/38           38
ge-1/1/39           39
ge-1/1/40           40
ge-1/1/41           41
ge-1/1/42           42
ge-1/1/43           43
ge-1/1/44           44
ge-1/1/45           45
ge-1/1/46           46
ge-1/1/47           47
ge-1/1/48           48
```

```
te-1/1/1            49
te-1/1/2            50
te-1/1/3            51
te-1/1/4            52
xe-1/1/1            53
xe-1/1/2            54
```

run show interface diagnostics tdr

The **run show interface diagnostics tdr** command.

Command Syntax

run show interface diagnostics tdr <*interface-name*>

Parameter

Parameter	Description
tdr <*interface-name*>	Specifies interface name of Ethernet electrical interface.

Example

- Run the following command to start the TDR cable test. The following example shows the cable length (Pair length) is approximately 31 meters long with a possible error of +/- 10 meters. All four pairs are working fine (Pair status).

```
admin@Xorplus# run show interface diagnostics tdr ge-1/1/1
Interface  Local pair Pair length(meter) Remote pair Pair status
---------- ---------- ------------------ ----------- -----------
ge-1/1/1   Pair A     31   +/- 10        Pair A      OK
           Pair B     31   +/- 10        Pair B      OK
           Pair C     31   +/- 10        Pair C      OK
           Pair D     30   +/- 10        Pair D      OK
```

Table 2. Description of the run show interface diagnostics tdr output

Item	Description
Interface	Indicates the name of the interface on which TDR test is enabled.
Local pair	Local four pairs.
Pair length(meter)	Displays the length and error of the cable pair in meters. • When the pair is not faulty, the Pair length in the displayed message refers to the total length of the pair. • When the pair is faulty, the Pair length in the displayed message is the length from the interface to the fault point in the cable.
Remote pair	Remote four pairs.
Pair status	The pair status could be "**OK**", "**OPEN**", "**SHORT**", "**OPENSHORT**", "**CROSSTALK**" or "**N/A**". • **OK**: indicates the link is up. • **OPEN**: indicates an open circuit, meaning a broken wire or maybe cable unplugged. • **SHORT**: indicates there is a short circuit on the cable. • **N/A**: indicates the port does not support TDR test.

interface max-route-limit

This command is to set max route count .

Command Syntax
set interface max-route-limit <*counter*>
delete interface max-route-limit

Parameter
•<*counter*> Max Route Counter,range is [0..12000]

Example
• This example is to set max route counter 12 and delete it:

```
admin@XorPlus# set interface max-route-limit 12
admin@XorPlus# delete interface max-route-limit
admin@XorPlus# commit
```

interface max-acl-rule-limit <egress/ingress>

This command is to set max acl rule counter .

Command Syntax
set interface max-acl-rule-limit <*egress/ingress*> <acl-counter>
delete interface max-acl-rule-limit egress
delete interface max-acl-rule-limit ingress

Parameter
• <*egress/ingress*> the in/out mode of a port

- **egress** Set max egress acl rule count
- **ingress** Set max ingress acl rule count

•<*acl-counter*> max egress or ingress acl counter identifier. Egress:,the counter is [0..256].ingress:[0..896]

Example
• This example is to max ingress ACL counter is 400

```
admin@XorPlus# set interface max-acl-rule-limit ingress 400
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> min_thresh

Users can set minimum thresh.

Command Syntax
set interface gigabit-ethernet <*port*> wred queue <*value*> min_thresh <*int*>
delete interface gigabit-ethernet <*port*> wred queue <*value*> min_thresh

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*value*> The queue number,[0..7]
•<*int*> The threshold identifier,[0..8000]

Example
• This example sets max thresh for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 min_thresh 1
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> max_thresh

Users can set max thresh.

Command Syntax
set interface gigabit-ethernet <*port*> wred queue <*value*> max_thresh <*int*>
delete interface gigabit-ethernet <*port*> wred queue <*value*> max_thresh

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*value*> The queue number,[0..7]
•<*int*> The threshold identifier,[0..8000]

Example
• This example sets max thresh for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 max_thresh 100
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> enable

Users can set wred queue when necessary.

Command Syntax
set interface gigabit-ethernet *<port>* wred queue *<value>* enable *<bool>*
delete interface gigabit-ethernet *<port>* wred queue *<value>* *enable*

Parameter
• *<port>*ethernet switching port identifier,the valid ports range 1-52
•*<value>* The queue number,[0..7]
•*<bool>* Set enable

- **true** enable wred
- **false** disable wred

Example
• This example sets wred queue for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 enable true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> ecn_thresh

Users can set ecn_thresh.

Command Syntax
set interface gigabit-ethernet <*port*> wred queue <*value*> ecn_thresh <*int*>
delete interface gigabit-ethernet <*port*> wred queue 2 ecn_thresh

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*value*> The queue number,[0..7]
•<*int*> The threshold identifier,[0..1],0 stands for disable ecn,1 stands for enable ecn.

Example
• This example sets ecn_thresh for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 ecn_thresh 0
admin@XorPlus# commit
```

interface gigabit-ethernet <port> wred queue <value> drop_probability

Users can set drop_probability.

Command Syntax
set interface gigabit-ethernet <*port*> wred queue <*value*> drop_probability <*int*>
delete interface gigabit-ethernet <port> wred queue <*value*> drop_probability

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*value*> The queue number,[0..7]
•<*int*> The probability identifier,[0...100]

Example
• This example sets wred queue drop probability for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 wred queue 2 drop_probability 10
admin@XorPlus# commit
```

interface gigabit-ethernet <port> storm-control <mode> ratio <value>

Users can set storm control mode for a specified port. The storm control function can control the rate of ingress traffic on the physical port. The ratio value is the percentage of the physical link speed.

Command Syntax
set interface gigabit-ethernet <*port*> storm-control <*mode*>*ratio* <*value*>
delete interface gigabit-ethernet <*port*> storm-control broadcast ratio

Parameter
• <*port*> ethernet port
• <*mode*> packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for all multicast traffic
- **unicast** Storm control for unknown unicast traffic

•<*value*> *range is* [0..100]. This value is percentage of the physical link speed. Note, when the value of the storm control is set to 0, it means that data packets are not allowed to pass.

Example
• This example set broadcast, multicast, unicast storm control for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast ratio 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control multicast ratio 20
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control unicast ratio 30
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus#
```

interface gigabit-ethernet <port> storm-control <mode> pps

Users can set storm control mode for a specified port.

Command Syntax
set interface gigabit-ethernet <*port*> storm-control <*mode*> pps <*value*>
delete interface gigabit-ethernet <*port*> storm-control [<*mode*> | **pps**]

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
• <*mode*> packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for multicast traffic
- **unicast** Storm control for unicast traffic

•<*value*> Packets per second, [0..30000000]. Note, when the value of the storm control is set to 0, it means that data packets are not allowed to pass.

Example
• This example set broadcast storm control for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast pps 1000
admin@XorPlus# commit
```

interface gigabit-ethernet <port> storm-control <mode> kbps

Users can set storm control mode for a specified port.

Command Syntax
set interface gigabit-ethernet <*port*> **storm-control** <*mode*> **kbps** <*value*>
delete interface gigabit-ethernet <*port*> **storm-control** [<*mode*> | **kbps**]

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
• <*mode*> packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for multicast traffic
- **unicast** Storm control for unicast traffic

•<*value*> Kilo bits per second, [0..10000000]. Note, when the value of the storm control is set to 0, it means that data packets are not allowed to pass.

Example
• This example set broadcast storm control for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 storm-control broadcast kbps 1000
admin@XorPlus# commit
```

interface gigabit-ethernet <port> static-ethernet-switching mac-address <mac-address> vlan <vlan-id>

User can configure a mac address for port belong to more than one vlan.

Command Syntax
set interface gigabit-ethernet <*port*> static-ethernet-switching mac-address <*mac-address*> vlan <*vlan-id*>

Parameter
• <*port*> GigabitEthernet IEEE 802.3z or 802.3ae. e.g. ge-1/1/1, ae1.
• <*mac-address*> Add static mac address for a specific interface.
• <*vlan-id*> VLAN tag identifier, the valid VLAN numbers range 1-4094, can create specify a range of VLAN numbers, e.g. 2,3,5-100.

Example
• This example configures a mac address for port belong to vlan 1.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 static-ethernet-switching mac-address 22:11:11:11:11:11 vlan
admin@XorPlus# commit
```

interface gigabit-ethernet <port> snmp-trap

Users can eable or disable snmp trap when necessary.

Command Syntax
set interface gigabit-ethernet <*port*> snmp-trap <*bool*>
delete interface gigabit-ethernet <*port*> snmp-trap

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
•<*bool*> Snmp trap when port link up and down

- **true** enable snmp-trap
- **false** disable snmp-trap

Example
• This example enable snmp-trap for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 snmp-trap true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> power-preemphasis-level

Users can set power-preemphasis-level for a port .

Command Syntax
set interface gigabit-ethernet <*port*> power-preemphasis-level <*value*>
delete interface gigabit-ethernet <*port*> power-preemphasis-level

Parameter
• <*port*>ethernet switching port identifier,the valid ports range 1-52
• <*value*>the level identifier, [0..15]

Example
• This example set preemphasis-level 3 for ge-1/1/1:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 power-preemphasis-level 3
admin@XorPlus# commit
```

interface gigabit-ethernet <port> mtu

Users can set maximum transmit packet size for a specified port.

Command Syntax
set interface gigabit-ethernet <*port*> mtu <*value*>
delete interface gigabit-ethernet <*port*> mtu

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52
• <*value*> maximum transmit packet size identifier(in octets),value is between [64..9216]

Example
• This example sets MTU 1024 for ge-1/1/3:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 mtu 1024
admin@XorPlus# commit
```

interface gigabit-ethernet <port> mac-learning <boolean>

This command function is setting if the port could learn the source mac address of ingress packet.

Command Syntax
set interface gigabit-ethernet <*port*> mac-learning <*boolean*>
delete interface gigabit-ethernet <*port*> mac-learning

Parameter
• <*port*> Ethernet switching port identifier
•<*boolean*> True or False. The default value is true. False value is the port can't learn the source mac address when packet is enterring the port. True value is the port can learn the source mac address.

Example
• This example configures the port ge-1/1/1 mac-learning false:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 mac-learning false
admin@XorPlus# commit
```

interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>

When local RS receive remote fault messages, local RS will inhibit transmission of frames.

These commands determine if local RS would ignore remote fault messages to permit transmission of frames when receiving remote fault messages.

Command Syntax

set interface gigabit-ethernet <port> link-fault-signaling ignore-remote-fault <boolean>.

Parameter

<port> Ethernet physical interface, now only support 10GE, 40GE, 100GE port .

<boolean> Vaule is false or true. Default value is false.

Example

This example is how to configure this command:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 link-fault-signaling ignore-remote-fault true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>

A fiber has two links, TX and RX. When RX link failure occurs, local fault messages are generated by PHY layer to RS layer. As soon as RS receives a local fault message, it will generate Remote fault messages and transmit Remote fault messages to remote RS through TX link. RS is the only layer that can generate Remote fault messages.

This command determines if local RS would ignore local fault message to generate Remote fault messages when RX link failure occurs. This command generally coordinates with another command of interface gigabit-ethernet <port> up-mode <boolean> when RX link of fiber breaks. If the two commands are configured together, TX link can still transmit traffic.

Command Syntax

set interface gigabit-ethernet <port> link-fault-signaling ignore-local-fault <boolean>

Parameter

• *<port>* Ethernet port, now only support 10GE, 40GE, 100GE port .

•*<boolean> Vaule is* false or true. Default value is false.

Example

• This example is how to configure this command:

```
admin@XorPlus# set interface gigabit-ethernet te-1/1/1 link-fault-signaling ignore-local-fault true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching vlan members <vlan-id> untagged

This command is to add a vlan member to the trunk port with untagged packet, vlan members range from 1 to 4094. When packets go out from this interface, the field of vlan tag will be removed from the packet.

Command Syntax
set interface gigabit-ethernet <*port*> family ethernet-switching vlan members <*vlan-id*> *untagged*
delete interface gigabit-ethernet <*port*> family ethernet-switching vlan members <*vlan-id*>

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
• <*vlan-id*> Configure vlan id for which the interface can carry traffic,eg:2,3...

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching vlan members 5 untagged
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching native-vlan-id

The native VLANID is the ID of the default VLAN (usually vlan-id 1) in which the the port belongs. User can change the native VLANID for port.

Command Syntax
set interface gigabit-ethernet <*port*> family ethernet-switching native-vlan-id <*vlan-id*>
delete interface gigabit-ethernet <*port*> family ethernet-switching native-vlan-id <*vlan-id*>

Parameter
• <*port*> Gigabit Ethernet IEEE 802.3z or 802.3ae. e.g. ge-1/1/1.
• <*vlan_id*> The native-vlan-id ,VLAN identifier to associate with untagged packets .the valid VLAN numbers range 1-4094.

Example
• This example creates VLAN 3 and puts ge-1/1/3 port on this VLAN:

```
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching native-vlan-id 3
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling mode

Users can configure a Q-in-Q tunnel mode for a port. By default, the mode is NONE.

Command Syntax
set interface gigabit-ethernet *<port>* family ethernet-switching dot1q-tunneling mode *[mode]*

Parameter
• *<port>* ethernet switching port identifier,the valid ports range 1-52.
• *[mode]* Q-in-Q tunnel mode.

- **internal** Flexible QinQ: service provider internal mode
- **external** Basic QinQ: customer to service provider mode
- **none** Disable tunneling mode,the **default** mode

Example
• This example is to set Q-in-Q tunnel mode for ge-1/1/3 port:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching dot1q-tunneling mode internal
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ingress

Users can configure/delete a Q-in-Q tunnel for entering traffic on a port.

Command Syntax
set interface gigabit-ethernet <*port*> family ethernet-switching dot1q-tunneling ingress <*text*>
delete interface gigabit-ethernet <*port*> family ethernet-switching dot1q-tunneling ingress <*text*>

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
• <*text*>Tunneling for entering traffic

Example
• This example is to configure a Q-in-Q tunnel for entering traffic:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching dot1q-tunneling ingress t2
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling ether-type

Users can set/delete a Ethertype value on Q-in-Q tunnel for a port.

Command Syntax
set interface gigabit-ethernet <*port*> family ethernet-switching dot1q-tunneling ether-type <*value*>
delete interface gigabit-ethernet <*port*> family ethernet-switching dot1q-tunneling ether-type <*value*>

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
• <value> Ethertype value

- **0x8100**
- **0x88a8**
- **0x9100**
- **0x9200**

Example
• This example is to select a Ethertype value on Q-in-Q tunnel for ge-1/1/3 port:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 family ethernet-switching dot1q-tunneling ether-type 0x8100
admin@XorPlus# commit
```

interface gigabit-ethernet <port> family ethernet-switching dot1q-tunneling egress

Users can configure/delete a Q-in-Q tunnel for exiting traffic on a port.

Command Syntax
set interface gigabit-ethernet <*port*> family ethernet-switching dot1q-tunneling egress <*text*>
delete interface gigabit-ethernet <*port*> family ethernet-switching dot1q-tunneling egress <*text*>

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
• <*text*>Tunneling for existing traffic

Example
• This example is to configure a Q-in-Q tunnel for existing traffic:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/4 family ethernet-switching dot1q-tunneling egress t2
admin@XorPlus# commit
```

interface gigabit-ethernet <port> disable

User can enable or disable an interface.

Command Syntax
set interface gigabit-ethernet <*port*> disable <*bool*>
delete interface gigabit-ethernet <*port*> disable

Parameter
• <*bool*> up/down an interface

- **true** disable an interface
- **false** enable an interface

Example
• This example is to disable ge-1/1/3 interface:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 disable true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> ether-options flow-control

Flow control is a mechanism used on Ethernet networks to slow the flow of traffic to prevent a receiving node from becoming overwhelmed. Implemented at the data link layer, it enables such a receiving node to send a message to other relevant switches or hosts to slow their data transfer rate. Ethernet flow control was originally implemented to address cases where network interface controllers (NICs) lacked sufficient buffer space to keep up with traffic flows. Today, it's more likely to be used to address network congestion in a switch, such as when traffic comes in over a higher speed link than the one where it goes out. It can also be useful when traffic is coming in from multiple high-speed connections and threatens to fill the switch buffer. This document details how to configure flow control on Gigabit Ethernet ports on a white box switch running the Pica8 PICOS network operating system.

Command Syntax
set interface gigabit-ethernet <*port*> ether-options flow-control <*bool*>
delete interface gigabit-ethernet <*port*> ether-options flow-control

Parameter
• <port> ethernet switching port identifier,the valid ports range 1-52
• <*bool*> enable flow control

- **true** enable flow control
- **false** disable flow control. This is default configuration.

Example
• This example is to configure ge-1/1/3 port in flow control:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 ether-options flow-control true
admin@XorPlus# commit
```

interface gigabit-ethernet <port> description

Users can add a description to a port.

Command Syntax
set interface gigabit-ethernet <*port*> description <*text*>
delete interface gigabit-ethernet <*port*> description

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52
• <*text*> Add a human-readable description of the interface

Example
• This example is to add description "hello" to ge-1/1/3.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 description hello
admin@XorPlus# commit
```

interface gigabit-ethernet <port> crossflow local-control

User can configure a crossflow port in local-control mode or not.

Command Syntax
set interface gigabit-ethernet <*port*> crossflow local-control <*bool*>
delete interface gigabit-ethernet <*port*> crossflow local-control

Parameter
• <*port*> a physical port or a LAG
• <*bool*> set local control

- **true** enable local control,**default** mode
- **false** disable local control

Example
• This example is to configure a croosflow port ge-1/1/3 not in local control:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 crossflow local-control false
admin@XorPlus# commit
```

interface gigabit-ethernet <port> crossflow enable

User can configure a specified port in crossflow mode or not.

Command Syntax
set interface gigabit-ethernet <*port*> crossflow enable <*bool*>
delete interface gigabit-ethernet <*port*> crossflow enable

Parameter
• <*port*> a physical port or a LAG
• <*bool*> Enable crossflow

- **true** enable crossflow
- **false** disable crossflow

Example
• This example is to configure ge-1/1/3 port in croosflow port:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 crossflow enable true
admin@XorPlus#commit
```

interface gigabit-ethernet <port> backup-port mode

User can set preemption mode of a port.

Command Syntax
set interface gigabit-ethernet <*port*> backup-port mode <*mode*>
delete interface gigabit-ethernet <*port*> backup-port mode

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
•<*mode*> Set preemption mode.

- **bandwidth** higher bandwidth interface preferred
- **forced** active interface preferred,the **default** mode
- **Off** turn off preemption

Example
• This example is to set the port preemption mode to bandwidth:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 backup-port mode bandwidth
admin@XorPlus# commit
```

interface gigabit-ethernet <port> backup-port interface

User can configure two physical ports or two LAGs as Flex Links, or one physical port and one LAG as Flex Links.

Command Syntax
set interface gigabit-ethernet <*port*> backup-port interface <*text*>
delete interface gigabit-ethernet <*port*> backup-port interface

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
•<*text*> Set backup port of an interface, which will disable rstp/mstp

Example
• This example is to set Flex links between a physical port and a LAG :

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 backup-port interface ae1
admin@XorPlus# commit
```

interface gigabit-ethernet <port> backup-port delay

User can set backup port delay time to a port.

Command Syntax
set interface gigabit-ethernet <*port*> backup-port delay <*seconds*>

Parameter
• <*port*> ethernet switching port identifier,the valid ports range 1-52.
•<*seconds*> preemption delay in seconds,range is [0..300]

Example
• This example is to set the delay time to 20s:

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/3 backup-port delay 20
admin@XorPlus# commit
```

interface ethernet-switching-options mac-table-aging-time

Users can configure the aging time of mac table

Command Syntax
set interface ethernet-switching-options mac-table-aging-time <*value*>
Delete interface ethernet-switching-options mac-table-aging-time

Parameter
• <*value*> Aging time in seconds, the range is [60..1000000].

Example
• This example is to configure the aging time (60)of mac table :

```
admin@XorPlus# set interface ethernet-switching-options mac-table-aging-time 60
admin@XorPlus# commit
```

interface ethernet-switching-options buffer queue-limit

interface ethernet-switching-options buffer queue-limit
User can set the limit value of queue buffer.

Command Syntax
set interface ethernet-switching-options buffer queue-limit <*value*>
delete interface ethernet-switching-options buffer queue-limit

Parameter
• <*value*>the queue-limit values indentifier,ranges from 0 to 20000

Example
• This example is to configure the buffer queue limit:

```
admin@XorPlus# set interface ethernet-switching-options buffer queue-limit 0
admin@XorPlus# delete interface ethernet-switching-options buffer queue-limit
admin@XorPlus#commit
```

interface ecmp max-path

This command is to set max counter of ecmp path.

Command Syntax
set interface ecmp max-path <*value*>
delete interface ecmp max-path

Parameter
•<*value*> Max of ecmp path

- **2**
- **4**
- **8**
- **16**
- **32**

Example
• This example is to set max of ecmp path 2:

```
admin@XorPlus# set interface ecmp max-path 2
admin@XorPlus# commit
```

interface cut-through-mode

Pica8 switch has two switching modes. One is store and-forward mode， another is cut-through mode.

By default, the switch forwards the packets in store and forward mode. Users can configure the switch to cut-through mode .

Command Syntax
set interface cut-through-mode <*bool*>
delete interface cut-through-mode

Parameter
• <*bool*> forwarding mode identifier

- **true** interface is in cut-through mode
- **false** interface is in store and forward mode

Example
• This example is to configure the interface in store and forward mode

```
admin@XorPlus# set interface cut-through-mode false
admin@XorPlus# commit
Merging the configuration.
Commit OK.
Save done.
XorPlus#
```

interface aggregate-ethernet <lag_name> storm-control <mode> pps

Users can set storm control mode for a specified port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **storm-control** <*mode*> **pps** <*value*>
delete interface aggregate-ethernet <*lag_name*> **storm-control broadcast pps**

Parameter
• <*lag_name*> Name of LAG interface.
• <*mode*> packets forwarding mode

- **broadcast** Storm control for broadcast traffic
- **multicast** Storm control for multicast traffic
- **unicast** Storm control for unicast traffic

•<*value*> Packets per second, [0..30000000]

Example
• This example set broadcast storm control for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 storm-control broadcast pps 1000
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> static-ethernet-switching mac-address <macaddr> vlan

Users can add static mac address for a specific LAG.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **static-ethernet-switching mac-address** <*macaddr*> **vlan** <*vlan-id*>
delete interface aggregate-ethernet <*lag_name*> **static-ethernet-switching mac-address** <*macaddr*> **vlan** <*vlan-id*>

Parameter
• <*lag_name*> Name of LAG interface.
•<*macaddr*> static mac address.
•<*vlan-id*> vlan identifier, the range is between 1 to 4094.

Example
• This example is to configure mac-addr 12:11:11:11:11:11 for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 static-ethernet-switching mac-address 12:11:11:11:11:11 vlan 1
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> snmp-trap

Users can eable or disable snmp trap when necessary.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **snmp-trap** <*bool*>
delete interface aggregate-ethernet <*lag_name*> **snmp-trap**

Parameter
• <*lag_name*> Name of LAG interface.
•<*bool*> Snmp trap when port link up and down

- **true** enable snmp-trap
- **false** disable snmp-trap

Example
• This example enable snmp-trap for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 snmp-trap true
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> mtu

Users can set maximum transmit packet size for a specified LAG.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **mtu** <*value*>
delete interface aggregate-ethernet <*lag_name*> **mtu**

Parameter
• <*lag_name*> Name of LAG interface.
• <*value*> maximum transmit packet size identifier(in octets),value is between 64 to 9216.

Example
• This example sets MTU to 1024 for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 mtu 1024
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> hash-mapping mode

This command is to control the data packets to forward on a specified LAG .

> NOTE：
>
> The configuration of this command takes effect only on known unicast traffic.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **hash-mapping mode** <*mode*>
delete interface aggregate-ethernet <*lag_name*> **hash-mapping mode**

Parameter
• <*lag_name*> Name of LAG interface.
•<*mode*> Configure hash mapping mode. The default value is **ethernet-source-destination**.

- **advance** Use global advanced configure as hash-key
- **advanced-resilient** Use resilient hashing with advanced configure as key
- **ethernet-destination-only** Use destination mac as hash-key
- **ethernet-source-destination** Use source and destination mac as hash-key
- **ethernet-source-only** Use source mac as hash-key
- **ip-destination-only** Use destination ip as hash-key
- **ip-source-destination** Use source and destination ip as hash-key
- **ip-source-only** Use source ip as hash-key

Example
• This example is configure hash mapping mode to ethernet-destination-only advance for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 hash-mapping mode ethernet-destination-only
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching native-vlan-id

The native VLANID is the ID of the default VLAN (usually vlan 1) in which the port belonged to. User can change the native VLANID for port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **family ethernet-switching native-vlan-id** <*vlan-id*>
delete interface aggregate-ethernet <*lag_name*> f**amily ethernet-switching native-vlan-id** <*vlan-id*>

Parameter
• <*lag*> Name of LAG interface.
• <*vlan_id*> The native-vlan-id ,VLAN identifier to associate with untagged packets .The valid VLAN number range is 1-4094.

Example
• This example creates VLAN 3 and puts ae1 on this VLAN:

```
admin@XorPlus# set vlans vlan-id 3
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching native-vlan-id 3
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling mode

Users can configure a Q-in-Q tunnel mode for a logical port. By default, the mode is none.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **family ethernet-switching dot1q-tunneling mode** <*mode*>

Parameter
• <*lag_name*> Name of LAG interface.
• *[mode]* Q-in-Q tunnel mode.

- external: customer mode
- internal: service provider mode
- none: Disable tunneling mode,default mode

Example
• This example is to set Q-in-Q tunnel mode for ae1 port:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling mode internal
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ingress

Users can configure/delete a Q-in-Q tunnel for inbound traffic on a logical port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **family ethernet-switching dot1q-tunneling ingress** <*text*>
delete interface aggregate-ethernet <*lag_name*> **family ethernet-switching dot1q-tunneling ingress** <*text*>

Parameter
• <*lag_name*> Name of LAG interface.
• <*text*>Tunneling for entering traffic

Example
• This example is to configure a Q-in-Q tunnel for inbound traffic on ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling ingress t2
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling ether-type

Set or delete an EtherType value on Q-in-Q tunnel for a logical port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **family ethernet-switching dot1q-tunneling ether-type** <*value*>

To delete enter:
delete interface aggregate-ethernet <*lag_name*> **family ethernet-switching dot1q-tunneling ether-type** <*value*>

Parameter
<*lag_name*> Name of LAG interface.
<value> EtherType value:

- **0x8100**
- **0x88a8**
- **0x9100**
- **0x9200**

Example
This example is to select a Ethertype value on Q-in-Q tunnel for ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling ether-type 0x8100
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> family ethernet-switching dot1q-tunneling egress

Configure or delete a Q-in-Q tunnel for outband traffic on a LAG.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **family ethernet-switching dot1q-tunneling egress** <*text*>

To delete the configuration enter:
delete interface gigabit-ethernet <*lag_name*> **family ethernet-switching dot1q-tunneling egress** <*text*>

Parameter
• <*lag_name*> Name of LAG interface.
• <*text*>*Q-in-Q t*unneling foroutband traffic.

Example
This example is to configure a Q-in-Q tunnel for egress logical port:

```
admin@XorPlus# set interface aggregate-ethernet ae1 family ethernet-switching dot1q-tunneling egress t2
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> crossflow local-control

Enable or disable local-control function of crossflow for a logical port.

Command Syntax
set interface aggregate-ethernet <*lag_name*> **crossflow local-control** <true | false**>**

To delete the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **crossflow local-control**

Parameter

- <*lag_name*> Name of LAG interface.
- true: enable local control, this is the default mode.
- false: disable local control

Example
The example disables local-control function of crossflow on port ae1.

```
admin@XorPlus# set aggregate-ethernet ae1 crossflow local-control false
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> crossflow enable

Enable or disable the crossflow mode in a logical port.

Command Syntax

set interface aggregate-ethernet <*lag_name*> **crossflow enable** <true | false>

To delete the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **crossflow enable**

Parameter

- <*lag_name*> Name of LAG interface.
- true: enable crossflow
- false: disable crossflow

Example

This example enables crossflow in ae1 port:

```
admin@XorPlus# set interface aggregate-ethernet ae1 crossflow enable true
admin@XorPlus#commit
```

interface aggregate-ethernet <lag_name> backup-port mode

User can set preemption mode of a logical port.

Command Syntax

set interface aggregate-ethernet <*lag_name*> **backup-port mode** <bandwidth | forced | Off>

To return to the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **backup-port mode**

Parameter

- <*lag_name*> Name of LAG interface.
- bandwidth: higher bandwidth interface preferred
- forced: active interface preferred,the default mode
- Off: turn off preemption

Example

This example is to set the port preemption mode to bandwidth:

```
admin@XorPlus# set interface aggregate-ethernet ae1 backup-port mode bandwidth
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> backup-port interface

User can configure two physical ports or two LAGs as Flex Links or one physical port and one LAG as Flex Links.

Command Syntax

set interface aggregate-ethernet <*lag_name*> **backup-port interface** <*interface_number*>

To return the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **backup-port interface**

Parameter

- <*lag_name*> Name of a configured LAG interface.
- <*interface_number*> Set backup port of an interface, which will disable RSTP/MSTP.

Example

This example is to set Flex links between a physical port and a LAG :

```
admin@XorPlus# set interface aggregate-ethernet ae1 backup-port interface ge-1/1/3
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> backup-port delay

Set backup port delay time, in seconds, to a port.

Command Syntax

set interface aggregate-ethernet <*lag_name*> **backup-port delay** <*seconds*>

To return the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **backup-port delay**

Parameter

- <*lag_name*> Name of a configured LAG interface.
- <*seconds*> Preemption delay, in seconds (range: 0 through 300 seconds)

Example

This example is to set the delay time to 20 seconds:

```
admin@XorPlus# set interface aggregate-ethernet ae1 backup-port delay 20
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> aggregated-ether-options min-selected-port

Configure min-selected-port for a specified logical port (LAG). Min-selected-port denotes that the LAG is up only when no fewer than the defined number of ports are up.

Command Syntax

set interface aggregate-ethernet <*lag_name*> **aggregated-ether-options min-selected-port** <*port-id*>

To return to the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **aggregated-ether-options min-selected-port**

Parameter

<lag_name>: Specifies a configured LAG interface name.
<port-id>: Minimum number of selected ports (range: **1** through **8**)

Example

This example is to configure min-selected-port for ae1.

```
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options min-selected-port 1
admin@XorPlus# commit
```

interface aggregate-ethernet <lag_name> aggregated-ether-options flow-control

Configure flow-control for a logical port.

> On N1148T-ON platform, flow control in the inbound direction of the interface is not supported.

Command Syntax

set interface aggregate-ethernet <*lag_name*> **aggregated-ether-options flow-control** <true | false>

To return the configuration enter:
delete interface aggregate-ethernet <*lag_name*> **aggregated-ether-options flow-control**

Parameter

- <*lag_name*>--Enter the name of the configured LAG interface.
- true: enable flow control
- false: disable flow control

Example

This example enables flow-control on the LAG ae1:

```
admin@XorPlus# set interface aggregate-ethernet ae1 aggregated-ether-options flow-control true
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field vlan disable

Use this command to enables aggregate load balancing hash map on the VLAN.

Command Syntax

set interface aggregate-balancing hash-mapping field vlan disable <true | false>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field vlan disable

Parameter

- **true**--disable vlan
- **false**--enable vlan

Example

This example is to enable ip-source:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field vlan disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field port-source disable

This command designates data packets to be forwarded via the port-source.

Command Syntax

set interface aggregate-balancing hash-mapping field port-source disable <true | false>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field port-source disable

Parameter

- **true**--disable port-source
- **false**--enable port-source

Example

This example enables data packets to be forwarded via ip-source:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field port-source disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field port-destination disable

This command designates data packets to be forwarded via the port-destination.

Command Syntax

set interface aggregate-balancing hash-mapping field port-destination disable <**true** | **false**>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field port-destination disable

Parameter

- **true**--disable port-destination
- **false**--enable port-destination

Example

This example enables data packets to be forwarded via port-destination:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field port-destination disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ip-source disable

This command designates data packets to be forwarded via the IP source.

Command Syntax

set interface aggregate-balancing hash-mapping field ip-source disable <**true** | **false**>

To return the configuration enter:
delete interface aggregate-balancing hash-mapping field ip-source disable

Parameter

- **true**--disable ip-source
- **false**--enable ip-source

Example

This example enables forwarding of data packets via ip-source:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ip-source disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ip-protocol disable

This command designates data packets to be forwarded via the IP protocol.

Command Syntax

set interface aggregate-balancing hash-mapping field ip-protocol disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ip-protocol disable

Parameter

- **true**--disable ip-protocol
- **false**--enable ip-protocol

Example

This example enables forwarding of data packets via the ip-protocol:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ip-protocol disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ip-destination disable

This command designates data packets to be forwarded via ip-destination.

Command Syntax

set interface aggregate-balancing hash-mapping field ip-destination disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ip-destination disable

Parameter

- **true**--disable ip-destination
- **false**--enable ip-destination

Example

This example enables data packet fowarded by ip-destination:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ip-destination disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ingress-interface disable

This command designates data packets to be forwarded via the ingress-interface.

Command Syntax

set interface aggregate-balancing hash-mapping field ingress-interface disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ingress-interface disable

Parameter

- **true--**disable ingress-interface
- **false--**enable ingress-interface

Example

This example enables ingress-interface:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ingress-interface disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ethernet-type disable

This command designates data packets to be forwarded via the ethernet-type.

Command Syntax

set interface aggregate-balancing hash-mapping field ethernet-type disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ethernet-type disable

Parameter

- **true**--disable ethernet-type
- **false**--enable ethernet-type

Example

This example enables data packets to be forwarded via ethernet-type:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ethernet-type disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ethernet-source-address disable

This command designates data packets to be forwarded via ethernet-source-address.

Command Syntax

set interface aggregate-balancing hash-mapping field ethernet-source-address disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ethernet-source-address disable

Parameter

- **true**--disable ethernet-source-address
- **false**--enable ethernet-source-address

Example

This example enables data packets to be forwarded via ethernet-source-address:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ethernet-source-address disable false
admin@XorPlus# commit
```

interface aggregate-balancing hash-mapping field ethernet-destination-address disable

This command designates data packets to be forwarded via the ethernet-destination-address.

Command Syntax

Set interface aggregate-balancing hash-mapping field ethernet-destination-address disable <**true** | **false**>

To remove the configuration enter:
delete interface aggregate-balancing hash-mapping field ethernet-destination-address disable

Parameter

- **true**--disable ethernet-destination-address
- **false**--enable ethernet-destination-address

Example

This example enables data packets forwarded by ethernet-destination-address:

```
admin@XorPlus# set interface aggregate-balancing hash-mapping field ethernet-destination-address disable false
admin@XorPlus# commit
```

set interface ecmp hash-mapping randomized-load-balancing

The **set interface ecmp hash-mapping randomized-load-balancing** command enables Randomized Load Balancing of ECMP (Equal-Cost Multi-Path Routing). That is to say, the next hop of the message is randomly generated among multiple equivalent routes.

The **delete interface ecmp hash-mapping randomized-load-balancing** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system reboot is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric** and **dlb-normal**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping randomized-load-balancing

delete interface ecmp hash-mapping randomized-load-balancing

Parameter

Null.

Example

- Enable Randomized Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping randomized-load-balancing
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping round-robin-load-balancing

The **set interface ecmp hash-mapping round-robin-load-balancing** command enables round robin mode of ECMP (Equal-Cost Multi-Path Routing) load balancing. That is, each equivalent route to the same destination address alternately forwards the traffic. For known unicast, if the packets have approximately the same length, you can choose to configure round-robin-based per-packet load balancing to achieve traffic load balancing.

The **delete interface ecmp hash-mapping round-robin-load-balancing** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system reboot is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric** and **dlb-normal**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping round-robin-load-balancing

delete interface ecmp hash-mapping round-robin-load-balancing

Parameter

Null.

Example

- Enable round robin mode of ECMP load balancing.

```
admin@PICOS# set interface ecmp hash-mapping round-robin-load-balancing
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping dlb-normal

The **set interface ecmp hash-mapping dlb-normal** command enables normal mode of Dynamic Load Balancing for ECMP (Equal-Cost Multi-Path Routing).

The **delete interface ecmp hash-mapping dlb-normal** command deletes the configuration.

- When the ECMP hash-mapping mode configuration (set/delete) changes, a system reboot is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric** and **dlb-normal**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping dlb-normal [**flowset-time** <*flowset-time*>]

delete interface ecmp hash-mapping dlb-normal

Parameter

Parameter	Description
flowset-time <*flowset-time*>	Optional. Specifies the inactive time interval for the flows. The value is an integer ranging from 16 to 32767 microseconds. The default value is 512 microseconds.

Usage Guidelines

After enabling the dynamic load sharing function, the traffic of Equal-Cost Multi-Path Routing (ECMP) can be distributed to different member links through dynamic load sharing, ensuring load balancing between member links.

Example

- Enable normal mode of Dynamic Load Balancing for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping dlb-normal
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

set interface ecmp hash-mapping symmetric

The **set interface ecmp hash-mapping symmetric** command enables Symmetric Hash for ECMP (Equal-Cost Multi-Path Routing) load balancing.

The **delete interface ecmp hash-mapping symmetric** command deletes the configuration.

- Make sure that the settings for the source IP and destination IP fields match, and that the settings for the source port and destination port fields match; otherwise symmetric hashing is disabled automatically.
- When the ECMP hash-mapping mode configuration (set/delete) changes, a system reboot is required for the configuration to take effect.
- ECMP hash-mapping modes (**round-robin-load-balancing**, **randomized-load-balancing**, **symmetric** and **dlb-normal**) are mutually exclusive. To switch between modes, you must first delete the configured mode before setting up the new one. Then, restart the system for the configuration to take effect.

Command Syntax

set interface ecmp hash-mapping symmetric <**true** | **false**>

delete interface ecmp hash-mapping symmetric

Parameter

Null.

Parameter	Description
<**true** | **false**>	Enables or disables Symmetric Hash for ECMP. The value could be **true** or **false**. • **true**: Enables Symmetric Hash for ECMP. • **false**: Disables Symmetric Hash for ECMP. The default value is **false**.

Example

- Enable Symmetric Hash for ECMP.

```
admin@PICOS# set interface ecmp hash-mapping symmetric true
admin@PICOS# commit
admin@PICOS# exit
admin@PICOS> request system reboot
```

VLAN Configuration Commands

This section contains descriptions of the CLI commands that this chapter references.

- set vlans dot1q-tunneling egress from
- set vlans dot1q-tunneling egress then action
- set vlans dot1q-tunneling egress then service-vlan
- set vlans dot1q-tunneling ingress from double-tag service-vlan
- set vlans dot1q-tunneling ingress from one-tag customer-vlan-list
- set vlans dot1q-tunneling ingress from untag enabled
- set vlans dot1q-tunneling ingress then
- set vlans vlan-id
- set vlans vlan-id description
- set vlans vlan-id l3-interface
- set vlans vlan-id vlan-name
- set vlans vlan-id private-vlan mode
- set vlans vlan-id private-vlan association
- set mac-map mac-address vlan
- run show vlans
- run show vlans private-vlan
- run show vlans private-vlan type
- run show mac-map
- set tracemac disable
- tracemac

set vlans dot1q-tunneling egress from

To configure tunneling for egress traffic, use the **set vlans dot1q-tunneling egress from** command in L2/L3 configuration mode. If the customer VLAN or service VLAN tag frame is specified, it can pass through the port.

Command Syntax

set vlans dot1q-tunneling egress *tunnel-id* **from** { **customer-vlan** | **service-vlan** } *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
customer-vlan	The customer VLAN identifier.
service-vlan	The service VLAN identifier.
vlan-id	VLAN identifier. The range is 0-4094.

Examples

This example configures tunneling *T0*, such that if the customer tag frame is 10 and the service tag frame is 100, the packet can pass through the port:

```
admin@Switch# set vlans dot1q-tunneling egress T0 from customer-vlan 10
admin@Switch# set vlans dot1q-tunneling egress T0 from service-vlan 100
```

set vlans dot1q-tunneling egress then action

To configure tunneling for egress traffic, use the **set vlans dot1q-tunneling egress then action** command in L2/L3 configuration mode. If a packet can pass through the port, it needs to be modified by the action.

Command Syntax

set vlans dot1q-tunneling egress *tunnel-id* **then action** { **change** | **none** | **one** | **two** }

Parameters

tunnel-id	Tunnel identifier.
change	Change the service VLAN tag.
none	Strip both the customer and service VLAN tags.
one	Retain the customer VLAN tag.
two	Retain both the customer and service VLAN tag.

Examples

This example explains how to configure the tunneling t5. If the packet can pass the port, the packet does not need to be changed.

- The service and customer tag frame of the packet need not to be removed

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action none
```

- The outside service tag frame of the packet need to be removed

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action one
```

- The service and customer tag frame of the packet need to be removed

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action two
```

- The service tag frame of the packet need to be replaced by 200

```
admin@XorPlus# set vlans dot1q-tunneling egress t5 then action change
admin@XorPlus# set vlans dot1q-tunneling egress t5 then service-vlan 200
admin@XorPlus# commit
```

set vlans dot1q-tunneling egress then service-vlan

To configure tunneling for egress traffic, use the **set vlans dot1q-tunneling egress then service-vlan** command in L2/L3 configuration mode. If a packet passes through the port, the service tag of the packet needs to be changed.

Command Syntax

set vlans dot1q-tunneling egress *tunnel-id* **then service-vlan** *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
vlan-id	VLAN identifier.

Examples

The following example shows how to configure *T0* tunneling. If a packet wants to pass through the port, the service tag of the packet needs to be replaced by 300:

```
admin@Switch# set vlans dot1q-tunneling egress T0 then service-vlan 300
```

set vlans dot1q-tunneling ingress from double-tag service-vlan

To configure tunneling for ingress traffic at a port, use the **set vlans dot1q-tunneling ingress from double-tag service-vlan** command in L2/L3 configuration mode. If a packet has double tags and service vlan is specified, the packet can pass through the port.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **from double-tag service-vlan** *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
vlan-id	VLAN identifier. The range is 0-4094.

Examples

The following example configures T0 tunneling for ingress traffic. If the packet has double tags and service vlan is 100, it can pass through the port:

```
admin@Switch# set vlans dot1q-tunneling ingress T0 from double-tag service-vlan 100
```

set vlans dot1q-tunneling ingress from one-tag customer-vlan-list

To configure tunneling for ingress traffic at a port, use the **set vlans dot1q-tunneling ingress from one-tag customer-vlan-list** command in L2/L3 configuration mode. If the packet has a single tag and customer VLAN is specified, it can pass through the port.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **from one-tag customer-vlan-list** *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
vlan-id	VLAN identifier.

Examples

The following example configures the tunneling *T1* for ingress traffic. If the packet has a single tag and customer VLAN is 10, it can pass through the port.

```
admin@Switch# set vlans dot1q-tunneling ingress T1 from one-tag customer-vlan-list 10
```

set vlans dot1q-tunneling ingress from untag enabled

To configure tunneling for untagged ingress traffic use the **set vlans dot1q-tunneling ingress from untag enabled** command in L2/L3 configuration mode.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **from untag enabled** { **true** | **false** }

Parameters

tunnel-id	Tunnel identifier.
true	Enable matching untagged traffic.
false	Disable matching untagged traffic.

Examples

The following configuration checks if untagged frames are received by the port or not:

```
admin@Switch# set vlans dot1q-tunneling ingress T1 from untag enabled true
admin@Switch# set vlans dot1q-tunneling ingress T1 from untag enabled false
```

set vlans dot1q-tunneling ingress then

To configure tunneling for ingress traffic received at a port and adding customer or service tag to frames, use the **set vlans dot1q-tunneling ingress then** command in L2/L3 configuration mode.

Command Syntax

set vlans dot1q-tunneling ingress *tunnel-id* **then** { **customer-vlan** | **service-vlan** } *vlan-id*

Parameters

tunnel-id	Tunnel identifier.
customer-vlan	The new customer VLAN identifier.
service-vlan	The new service VLAN identifier.
vlan-id	VLAN identifier. The range is 0-4094.

Examples

The following example configures the T0 tunneling to add customer tag 10 and service tag 100 to frames:

```
admin@Switch# set vlans dot1q-tunneling ingress T0 then customer-vlan 10
admin@Switch# set vlans dot1q-tunneling ingress T0 then service-vlan 100
```

set vlans vlan-id

The command set vlans vlan-id can be used to create a VLAN. Vlan-id 1 exists by default.

> **NOTE:**
> VLAN IDs (VLAN 1-4094) have been pre-configured in the system from version 4.3.2 and are not user-deletable. Users no longer need to use command **set vlans vlan-id** <*vlan-id*> to create VLAN IDs.

Command Syntax
set vlans vlan-id <*vlan-id*>
delete vlans vlan-id <*vlan-id*>

Parameter
• <*vlan_id*> VLAN tag identifier. The valid VLAN numbers range 1-4094. User can specify a range of VLAN numbers, e.g. 2,3,5-100.

Example
• This example creates VLAN 10:

```
admin@XorPlus# set vlans vlan-id 10
admin@XorPlus# commit
```

set vlans vlan-id description

To add description for a VLAN, use the **set vlans vlan-id description** command in L2/L3 configuration mode.

Command Syntax

set vlans vlan-id *vlan-id* **description** *description*
delete vlans vlan-id *vlan-id* **description**

Parameters

vlan-id	VLAN identifier. The range of values is from 1 to 4094. A range of VLAN identifiers can be specified, for example, 2,3,5-100.
description	VLAN description in free text format.

Example

The following example creates description for VLAN 10:

```
admin@Switch# set vlans vlan-id 10 description "My Favorite VLAN"
```

set vlans vlan-id l3-interface

To associate a Layer 3 interface with a VLAN, use the **set vlans vlan-id l3-interface** command. To remove the Layer 3 interface, use the **delete** form of the command.

Command Syntax

set vlans vlan-id *vlan-id* **l3-interface** *interface-name*
delete vlans vlan-id *vlan-id* **l3-interface**

Parameters

vlan-id	VLAN identifier. The range of allowed VLAN identifiers is 1-4094. A range of VLAN identifiers can be used, for example, 2,3,4,5-100.
interface-name	Name of the Layer 3 interface.

Example

- This example associates a Layer 3 interface vlan-1 with VLAN 10 and then removes the Layer 3 interface from the VLAN:

```
admin@Switch# set vlans vlan-id 10 l3-interface vlan-1
admin@Switch# commit
admin@Switch# delete vlans vlan-id 10 l3-interface
admin@Switch# commit
```

set vlans vlan-id vlan-name

To create a VLAN, use the **set vlans vlan-id** command in L2/L3 configuration mode. To give a name to the VLAN, use the optional **vlan-name** keyword. To remove a VLAN, use the **delete** form of the command.

Command Syntax

set vlans vlan-id *vlan-id* [**vlan-name** *vlan-name*]
delete vlans vlan-id *vlan-id*

Parameters

vlan-id	VLAN identifier. The range is from 1 to 4094. A range of VLAN identifiers can be specified, for example, 2,3,5-100.
vlan-name	VLAN name. Up to 32 alphanumeric characters in length.

Example

This example creates VLAN 10 and names it MyVLAN:

```
admin@Switch# set vlans vlan-id 10 vlan-name MyVLAN
```

set vlans vlan-id private-vlan mode

The **set vlans vlan-id private-vlan mode** command configures the PVLAN mode of a VLAN.

Command Syntax

set vlans vlan-id <*vlan-id*> **private-vlan mode** <**primary** | **community** | **isolated**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
private-vlan mode <**primary**	**community**	**isolated**>	Specifies the PVLAN mode of a VLAN. The value could be **primary**, **community** or **isolated**. • **primary**: Configures a VLAN as a primary VLAN. • **community**: Configures a VLAN as a community VLAN. • **isolated**: Configures a VLAN as an isolated VLAN.

Usage Guidelines

PVLAN function involves the following VLAN types:

- Primary VLAN: allows member interfaces to communicate with each other and with interfaces in secondary VLANs.
- Secondary VLAN
- Isolated VLAN: allows member interfaces to communicate with only interfaces in the primary VLAN. An interface in an isolated VLAN cannot communicate with interfaces in the same VLAN or other secondary VLANs.
- Community VLAN: allows member interfaces to communicate with each other within the same VLAN and interfaces in the primary VLAN. An interface in a secondary VLAN cannot communicate with interfaces in other secondary VLANs.

NOTE:

If you want to change a private VLAN to a normal VLAN, you need to remove the configurations for PVLAN-related binding relationship before you can remove the PVLAN mode configuration. For example, if you use the **set vlans vlan-id** <*vlan-id*> **private-vlan association** <*secondary-vlan-list*> command for PVLAN association, remove the binding relationship first before you can change the private VLAN to a normal VLAN.

Similarly, it also requires to remove the private VLAN relevant configuration before changing the role of a private VLAN to another PVLAN type, e.g. when changing the PVLAN type from primary VLAN to secondary VLAN.

Example

- Configure a primary VLAN.

```
admin@Xorplus# set vlans vlan-id 2 private-vlan mode primary
admin@Xorplus# commit
```

set vlans vlan-id private-vlan association

The **set vlans vlan-id private-vlan association** command associates the secondary VLAN list with the primary VLAN.

Command Syntax

set vlans vlan-id <*vlan-id*> **private-vlan association** <*secondary-vlan-list*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies the primary VLAN ID. The value is an integer.
<*secondary-vlan-list*>	Specifies secondary VLAN list in a primary VLAN. The value is a string. E.g. 3, 5, 100-200. The VLANs in the list need to be previously configured as either an isolated VLAN or a community VLAN.

Usage Guidelines

Configure the association between primary VLAN and secondary VLAN list to specify a PVLAN pair.

NOTE:

- Before setting this command, use command set vlans vlan-id <*vlan-id*> private-vlan mode <primary | community | isolated> to configure the PLAN types.
- A primary VLAN can be associated with multiple community VLANs and only one isolated VLAN.
- A secondary VLAN (isolated or community) can be associated with only one primary VLAN.
- If you run this command with the same primary VLAN multiple times, only the latest configuration takes effect.
- Before modifying or deleting PVLAN association configuration, you need to delete all the PVLAN settings of the involved Private VLANs.

Example

- Associate the secondary VLAN list 2-3 with the primary VLAN 5.

```
admin@Xorplus# set vlans vlan-id 5 private-vlan association 2-3
admin@Xorplus# commit
```

set mac-map mac-address vlan

The **set mac-map mac-address vlan** command configures MAC address and VLAN mapping entry.

The **delete mac-map mac-address vlan** command deletes the configuration.

> **NOTE:**
> The same MAC address can be bound to no more than one VLAN.

Command Syntax

set mac-map mac-address <*mac-address*> **vlan** <*vlan-id*>

Parameters

Parameter	Description
mac-address <*mac-address*>	Specifies a MAC address binding to the VLAN. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. MAC address cannot be set to all-0, all-F or multicast address.
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1-4094.

Example

- Configure MAC address 00:22:22:22:22:20 to VLAN 200 mapping entry.

```
admin@Xorplus# set mac-map mac-address 00:22:22:22:22:20 vlan 200
admin@Xorplus# commit
```

run show vlans

The **run show vlans** command displays information about VLANs configured on a switch. With the command display VLANID, Tag, and Interface by default, user can display the brief, detail or special VLANID information.

Command Syntax

run show vlans <*text*>

Parameter

• <*text*> The specific information, options include:

- **brief** Show vlan brief information
- **detail** Show vlan detail information
- **vlan-id** <*vlan-id*> Show specific vlan detail information

Example

• This example shows VLAN 10:

```
admin@XorPlus# run show vlans
VlanID Vlan Name  Tag      Interfaces
------ --------   -------- ------------------------------------------------------
1      default    untagged ge-1/1/2, ge-1/1/3, ge-1/1/4, ge-1/1/5, ge-1/1/6
                           ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10, ge-1/1/11
                           ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15, ge-1/1/16
                           ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20, ge-1/1/21
                           ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25, ge-1/1/26
                           ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30, ge-1/1/31
                  tagged
10     aaa        untagged ge-1/1/1
                  tagged

admin@XorPlus# run show vlans vlan-id 10
VLAN ID: 10
VLAN Name: aaa
Description: myvlan
vlan-interface:
Routed-interface:
Number of member ports: 1
Untagged port: 1
Tagged port: None
```

run show vlans private-vlan

The **run show vlans private-vlan** command shows the PVLAN configuration information.

Command Syntax

run show vlans private-vlan

Parameter

Null.

Example

- View the PVLAN configuration information.

```
admin@Xorplus# run show vlans private-vlan
Primary   Secondary  Type            Tag         Interfaces
-------   ---------  -----------     --------    -------------------------
5                    primary         untagged    te-1/1/1
                                       tagged
          2          isolated        untagged    ge-1/1/1, ge-1/1/2
                                       tagged
          3          community       untagged    ge-1/1/3, ge-1/1/4
                                       tagged
```

The field “**Tag**” indicates whether the packets will be tagged or not when they are sent from this port.

run show vlans private-vlan type

The **run show vlans private-vlan type** command is used to view the PVLAN type information.

Command Syntax

run show vlans private-vlan type

Parameter

Null.

Example

- View the PVLAN type information.

```
admin@Xorplus# run show vlans private-vlan type
Vlan Type
---- -----------
5    primary
2    isolated
3    community
```

run show mac-map

The **run show mac-map** command is used to view the configuration information of MAC-based VLAN.

Command Syntax

run show mac-map [**mac-address** <*mac-address*>]

Parameter

Parameter	Description
mac-address <*mac-address*>	Optional. Specifies a MAC address binding to the VLAN. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Example

- View the configuration information of MAC-based VLAN.

```
admin@Xorplus# run show mac-map
Total entries: 4096
MAC               VLAN
00:33:33:33:33:20  400
00:22:22:22:22:20  300

admin@Xorplus# run show mac-map mac-address 00:22:22:22:22:20
MAC               VLAN
00:22:22:22:22:20  300
```

set tracemac disable

The **set tracemac disable** command can be used to enable or disable MAC trace function.

The **delete tracemac disable** command deletes the configuration.

Command Syntax

set tracemac disable <**true | false**>

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable MAC trace function. The value could be **true** or **false**. • **true**: Disable MAC trace function. • **false**: Enable MAC trace function. By default, MAC trace function is disabled.

Example

- Enable MAC trace function.

```
admin@PICOS# set tracemac disable false
admin@PICOS# commit
```

tracemac

The **tracemac** command output shows the Layer 2 path connectivity between the current device and the destination device.

Command Syntax

run tracemac destination <*mac-address*> **vlan** <*vlan-id*>

Parameters

Parameter	Description
destination <*mac-address*>	Specifies a MAC address. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. MAC address cannot be set to all-0, all-F or multicast address.
vlan <*vlan-id*>	Specifies the VLAN ID of the destination MAC. The value is an integer that ranges from 1-4094.

Example

- Trace MAC destination device with MAC address 20:11:11:11:11:11:11 and belonging to VLAN 100.

```
admin@PICOS# run tracemac destination 22:11:11:11:11:11 vlan 4094
Hop   Hostname    Ingress port   Ingress mac        Egress port   Egress mac
----- ----------- -------------- ------------       ------------  ------------
1     PICOS       xe-1/1/1.1     70:72:cf:b7:65:45  te-1/1/5      70:72:cf:b7:65:45
2     PICOS       te-1/1/3       04:f8:f8:20:6c:7b  -             04:f8:f8:20:6c:7b
```

NOTE:

The ingress port in the output of the command only displays the member port of the LAG port.

Voice VLAN Configuration Commands

- set interface gigabit-ethernet voice-vlan mode
- set interface gigabit-ethernet voice-vlan tagged mode
- set interface gigabit-ethernet voice-vlan vlan-id
- set vlans voice-vlan aging
- set vlans voice-vlan dscp
- set vlans voice-vlan local-priority
- set vlans voice-vlan mac-address mask
- set vlans voice-vlan mac-address description
- show vlans voice-vlan
- show vlans voice-vlan oui
- show vlans voice-vlan vlan-id <text>

set interface gigabit-ethernet voice-vlan mode

The **set interface gigabit-ethernet voice-vlan mode** command configures the mode in which an interface is added to a voice VLAN.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **voice-vlan mode** <**auto** | **manual**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical port of the switch.
mode <**auto**	**manual**>	Specifies the mode in which an interface is added to a voice VLAN.The value is **auto** or **manual**. • **auto**: indicates the automatic mode. • **manual**: indicates the manual mode. The default value is **auto**.

Usage Guidelines

Auto and manual mode determine the mode of the port when added to the voice VLAN.

- **Auto Mode**

In automatic mode, the system uses the protocol packets sent by the IP phone. If the source MAC address of the packets matches the OUI address, the system will automatically add the ingress port of the voice packet to the voice VLAN, and then install the ACL rules of voice VLAN and implement the priority of the packet. If the source MAC address of the packets matches no OUI address, the system will learn the source MAC address of the LLDP, LLDP-MED or CDP packet as the learned OUI and add the port to the voice VLAN.

You can set the voice VLAN aging time on the device. During the aging time, if no voice packet is received from the ingress port, the system deletes the port from the voice VLAN. The process of adding/deleting a port to the voice VLAN is implemented automatically by the system.

- **Manual Mode**

In manual mode, the port is added to voice VLAN manually. This type of port is not affected by the aging time of the voice VLAN. When the aging time expires, it is not deleted from the voice VLAN.

In manual mode, the ports is added to voice VLAN by manual configuration. If the source MAC address of the packets matches the OUI address, the system will install the ACL rules of voice VLAN and implement the priority of the packet. The process of adding/deleting a port to the voice VLAN is implemented manually by the administrator.

Example

- Configure interface ge-1/1/1 be added to the voice VLAN in auto mode.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 voice-vlan mode auto
admin@Xorplus# commit
```

set interface gigabit-ethernet voice-vlan tagged mode

The **set interface gigabit-ethernet voice-vlan tagged mode** command configures the tagged mode for the outgoing packet of a voice VLAN interface.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **voice-vlan tagged mode** <**tag | untag | auto**>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical port of the switch.
tagged mode <tag | untag | auto>	Configure the tagged mode for the outgoing packet of a voice VLAN interface. The value could be **tag**, **untag** or **auto**. • **tag**: the outgoing packets of a voice VLAN interface be tagged with the voice VLAN ID regardless of the protocol type used between the switch and the IP phone. • **untag**: the outgoing packets of a voice VLAN interface be untagged regardless of the protocol type used between the switch and the IP phone. • **auto**: the system automatically determines whether the outgoing packet of a voice VLAN interface be tagged with the voice VLAN ID per the protocol type. The value **auto** is the default and recommended value.

Usage Guidelines

For tagged mode auto,

- If the packet matches the user defined OUI addresses or the OUI addresses learned from CDP and LLDP protocols, the outgoing packet from a voice VLAN interface will be untagged when the tagged mode is auto.
- If the packet matches the OUI addresses learned from LLDP-MED protocol, the outgoing packet of a voice VLAN interface will be tagged with the voice VLAN ID based on the result of the LLDP-MED protocol negotiation between the switch and the IP phone when the tagged mode is auto.
  - If the negotiation result of LLDP-MED protocol between the switch and the IP phone is SUCCESS, the outgoing packet of a voice VLAN interface will be tagged with the voice VLAN ID.
  - Else if the negotiation result of LLDP-MED protocol between the switch and the IP phone is FAILURE, the outgoing packet of a voice VLAN interface will be untagged.

Example

- Configure the outgoing packet of a voice VLAN interface ge-1/1/1 be tagged with the voice VLAN ID.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 voice-vlan tagged mode tag
admin@Xorplus# commit
```

set interface gigabit-ethernet voice-vlan vlan-id

The **set interface gigabit-ethernet voice-vlan vlan-id** command configures an interface into voice VLAN.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **voice-vlan vlan-id** <*vlan-id*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the physical port of the switch to be added to voice VLAN.
vlan-id <*vlan-id*>	Specifies a voice VLAN ID.

Example

- Configure interface ge-1/1/1 into voice VLAN 10.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 voice-vlan vlan-id 10
admin@Xorplus# commit
```

set vlans voice-vlan aging

The **set vlans voice-vlan aging** command configures the aging time for voice VLAN.

Command Syntax

set vlans voice-vlan aging <*aging-time*>

Parameter

Parameter	Description
aging <*aging-time*>	Specifies the aging time for voice VLAN. The value is an integer, in minutes, that ranges from 5 to 43200. The default value is 1440.

Usage Guidelines

You can set the voice VLAN aging time on the device. Until the aging time expires, if no voice packet is received from the ingress port, the system deletes the port from the voice VLAN.

- For the OUI of dynamic learning, when a LLDP neighbor entry in the MAC address table has aged, the aging time of voice VLAN starts. LLDP neighbor entry aging time is the “Time To Live” value in the received LLDP packet.
- For static OUI, when a MAC entry in the MAC address table has aged, the aging time of voice VLAN starts. The status of voice VLAN switches from working to aging, if no voice packet corresponding to the OUI is received until the aging timer expires, the status of voice VLAN switches from aging to idle. After which the learned OUI is cleared and the port is removed from the voice VLAN.

NOTE:

The voice VLAN aging time works only on auto mode.

Example

- Configure the aging time for voice VLAN to 30 minutes.

```
admin@Xorplus# set vlans voice-vlan aging 30
admin@Xorplus# commit
```

set vlans voice-vlan dscp

The **set vlans voice-vlan dscp** command modifies the DSCP value for the voice VLAN.

Command Syntax

set vlans voice-vlan dscp <*dscp-value*>

Parameter

Parameter	Description
dscp <*dscp-value*>	Specifies the DSCP value for the voice VLAN. The value is an integer that ranges from 0 to 63.

Usage Guidelines

Differentiated Services Code Point (DSCP) value is used to provide Diff-Serv (Differentiated Service) node behavior for the specified application type as defined in IETF RFC 2474. This 6 bit field may contain one of 64 code point values (0 through 63). The six bits Type of Service (TOS) field in the IPv4 data packet header are used for DSCP.

Example

- Configure the DSCP value to 50 for the voice VLAN.

```
admin@Xorplus# set vlans voice-vlan dscp 50
admin@Xorplus# commit
```

set vlans voice-vlan local-priority

The **set vlans voice-vlan local-priority** command modifies the 802.1p priority for the voice VLAN.

Command Syntax

set vlans voice-vlan local-priority <*priority-value*>

Parameter

Parameter	Description
local-priority <*priority-value***>**	Specifies the 802.1p priority for the voice VLAN. The value is an integer that ranges from 0 to 7.

Usage Guidelines

802.1p priority is the value of the priority field in the VLAN frame in IEEE 802.1Q standard, which contains the layer 2 priority to be used for the specified application type. This 3 bit field could specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004.

This configuration not only changes the 802.1p priority value in the packet, but also changes egress queue of the packet.

Example

- Configure the 802.1p priority to 7 for the voice VLAN.

```
admin@Xorplus# set vlans voice-vlan local-priority 7
admin@Xorplus# commit
```

set vlans voice-vlan mac-address mask

The **set vlans voice-vlan mac-address mask** command configures the OUI address for the voice VLAN.

Command Syntax

set vlans voice-vlan mac-address <*mac-address***> mask** <*oui-mask*>

Parameter

Parameter	Description
mac-address <*mac-address***>**	Specifies the OUI address for voice VLAN. The value is in H:H:H:H:H:H format. An H contains 2 hexadecimal numbers. The address cannot be all 0s, multicast address, or broadcast address.
mask <*oui-mask***>**	Specifies the mask for the OUI address.

Usage Guidelines

OUI refers to the first 24 bits (binary) of the MAC address that can be used to represent a MAC address segment, which is a globally unique identifier assigned by the IEEE to different device vendors, each device vendor then allocates 24 bit to form a 48-bit MAC address.

In voice VLAN, the OUI is not necessarily 24 bits long which depends on the mask value. The OUI is the result of the AND operation between the MAC address and the mask in the **set vlans voice-vlan mac-address mask** command.

The switch identifies packets as voice data when the source MAC address matches the system pre-configured Organizationally Unique Identifier (OUI).

NOTE:

The system supports a maximum of 10 OUIs, including the default 7 OUIs. In PICOS 2.11.4 and the later version , there is no default OUI, the user is allowed to configure a maximum of 10 OUIs.

Example

- Configure an OUI address for the voice VLAN.

```
admin@Xorplus# set vlans voice-vlan mac-address 00:11:11:00:00:01 mask ff:ff:ff:00:00:00
admin@Xorplus# commit
```

set vlans voice-vlan mac-address description

The **set vlans voice-vlan mac-address mask** command configures the description information for the OUI address.

Command Syntax

set vlans voice-vlan mac-address <*mac-address***> description** <*text*>

Parameter

Parameter	Description
mac-address <*mac-address***>**	Specifies the OUI address for voice VLAN. The value is in H:H:H:H:H:H format. An H contains 2 hexadecimal numbers. The address cannot be all 0s, multicast address, or broadcast address.
description <*text***>**	Optional. Add the description information for the OUI address. The value is a string.

Example

- Configure the description information for the OUI address.

```
admin@Xorplus# set vlans voice-vlan mac-address 00:11:11:00:00:01 description CompanyPhone
admin@Xorplus# commit
```

show vlans voice-vlan

Show voice vlan detail information.

Command Syntax
show vlans voice-vlan

Description

Generally speaking, what the command shows contains two logical parts.

1.OUI

This part shows all the oui addresses and their mask and description.

```
Oui_Address          Mask                Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0      Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0      Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0      Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0      Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0      Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0      Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0      3com phone
```

2.Specified voice-vlan id

The following example contains 4 voice-vlans. Let's take voice-vlan id:10 for example.

```
Voice Vlan ID:10
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/1       auto      false                      Aging:86274sec
```

- Voice Vlan ID: 10 means the voice-vlan id is 10
- The following 3 items is global parameters, local priority, dscp and aging time is the same in all the 4 voice-vlans

```
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
```

- Port means the ports below are configured this voice-vlan id.
- Mode means voice-vlan mode of the port: auto or manual.
- Tagged means the outgoing packets with OUI source Mac-address from the port will be tagged of not. It has two values: true and false. True means tagged and false means untagged.
- Mac_address displays OUI source Mac-address the port has learned. It shows the result of Oui_Address AND mask.
- Status shows the voice-vlan working status of the port.

Status of Voice Vlan	Description
Aging:<text>sec	Only auto mode has this status. This port won't be in this vlan after <text> seconds.
Working	Voice vlan is working on the port. The port is in the vlan(voice-vlan id).
Idle	Only auto mode has this status, voice vlan is not working on the port.

Example
• This example is to show voice-vlan detail information, ge-1/1/1 is auto mode and aging, ge-1/1/2 is auto mode and working, ge-1/1/3 is auto mode but not working, ge-1/1/4 is manual mode

```
admin@XorPlus# run show vlans voice-vlan
Oui_Address          Mask                Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0      Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0      Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0      Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0      Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0      Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0      Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0      3com phone
Voice Vlan ID:10
Voice Vlan local priority:6
Voice Vlan dscp:46
```

```
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/1       auto      false                      Aging:86274sec
Voice Vlan ID:20
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/2       auto      false     0:1:e3:0:0:0     Working
Voice Vlan ID:30
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/3       auto      false                      Idle
Voice Vlan ID:40
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/4       manual    false                      Working
```

show vlans voice-vlan oui

Show voice vlan oui detail information, including default oui, static oui and oui learned from LLDP packet.

Command Syntax
show vlans voice-vlan oui

Default OUI as below :

```
Oui_Address          Mask                Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0      Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0      Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0      Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0      Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0      Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0      Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0      3com phone
```

OUI Learned from LLDP packet as below :

```
LLDP_Oui_Address     Mask
22:22:22:22:22:33    ff:ff:ff:ff:ff:ff
22:22:22:22:22:44    ff:ff:ff:ff:ff:ff
```

LLDP are deployed between pica8 switch and IP phone. This command can't show LLDP OUI address when switch doesn't receive any LLDP packet from IP phone.

Example

• This example is to show voice-vlan oui detail information::

```
admin@XorPlus# run show vlans voice-vlan oui
Oui_Address          Mask                Description
0:1:e3:0:0:0         ff:ff:ff:0:0:0      Siemens phone
0:3:6b:0:0:0         ff:ff:ff:0:0:0      Cisco phone
0:4:d:0:0:0          ff:ff:ff:0:0:0      Avaya phone
0:60:b9:0:0:0        ff:ff:ff:0:0:0      Philips/NEC phone
0:d0:1e:0:0:0        ff:ff:ff:0:0:0      Pingtel phone
0:e0:75:0:0:0        ff:ff:ff:0:0:0      Polycom phone
0:e0:bb:0:0:0        ff:ff:ff:0:0:0      3com phone
22:33:44:0:0:0       ff:ff:ff:0:0:0      user1

LLDP_Oui_Address     Mask
22:22:22:22:22:33    ff:ff:ff:ff:ff:ff
22:22:22:22:22:44    ff:ff:ff:ff:ff:ff
```

show vlans voice-vlan vlan-id <text>

Show special voice vlan id detail information.

Command Syntax
show vlans voice-vlan vlan-id <text>

Parameter
•<text> voice-vlan id, can't be the same with pvid or vlan-member

Example
• This example is to show voice-vlan detail information::

```
1.ge-1/1/1 is in suto mode and aging.
admin@XorPlus#  run show vlans voice-vlan vlan-id 10
Voice Vlan ID:10
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/1       auto      false                      Aging:86143sec

2.ge-1/1/2 is in auto mode and working.
admin@XorPlus# run show vlans voice-vlan vlan-id 20
Voice Vlan ID:20
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/2       auto      false     0:1:e3:0:0:0     Working

3.ge-1/1/3 is in auto mode and not working.
admin@XorPlus# run show vlans voice-vlan vlan-id 30
Voice Vlan ID:30
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/3       auto      false                      Idle

4.ge-1/1/4 is in manual mode. It can't display any mac-addresses and status will always be working in this mode.
admin@XorPlus# run show vlans voice-vlan vlan-id 40
Voice Vlan ID:40
Voice Vlan local priority:6
Voice Vlan dscp:46
Voice Vlan aging time:1440 minutes
Current voice vlan enabled port mode:
Port           Mode      Tagged    Mac_Address      Status
-------------------------------------------------------------------
ge-1/1/4       manual    false                      Working
```

Layer 3 Routing Commands

- run show neighbors
- run show route
- run show route forward-host
- run show route forward-route
- run show vrf
- set ip vrf
- set ip routing enable
- set system management-vrf enable
- BGP Commands
  - run show bgp
  - run show bgp neighbor
  - run show bgp route
  - run show bgp unicast neighbor graceful-restart
  - set protocols bgp aggregate-address
  - set protocols bgp always-compare-med
  - set protocols bgp bestpath as-path type multipath-relax
  - set protocols bgp bestpath bandwidth
  - set protocols bgp bestpath compare-routerid
  - set protocols bgp bestpath med missing-as-worst
  - set protocols bgp cluster-id
  - set protocols bgp graceful-shutdown
  - set protocols bgp listen
  - set protocols bgp local-as
  - set protocols bgp max-med
  - set protocols bgp multipath maximum-paths
  - set protocols bgp neighbor activate
  - set protocols bgp neighbor addpath-tx-all-paths
  - set protocols bgp neighbor addpath-tx-bestpath-per-as
  - set protocols bgp neighbor advertisement-interval
  - set protocols bgp neighbor allowas-in
  - set protocols bgp neighbor as-override
  - set protocols bgp neighbor capability extended-nexthop
  - set protocols bgp neighbor default-originate
  - set protocols bgp neighbor description
  - set protocols bgp neighbor disable-connected-check
  - set protocols bgp neighbor ebgp-multihop
  - set protocols bgp neighbor filter-list
  - set protocols bgp neighbor next-hop-self
  - set protocols bgp neighbor password
  - set protocols bgp neighbor peer-group
  - set protocols bgp neighbor prefix-list
  - set protocols bgp neighbor remote-as
  - set protocols bgp neighbor remove-private-as
  - set protocols bgp neighbor route-map
  - set protocols bgp neighbor route-reflector-client
  - set protocols bgp neighbor send-community
  - set protocols bgp neighbor shutdown
  - set protocols bgp neighbor soft-reconfiguration
  - set protocols bgp neighbor timers connect
  - set protocols bgp neighbor timers holdtime
  - set protocols bgp neighbor timers keepalive
  - set protocols bgp neighbor ttl-security hops
  - set protocols bgp neighbor update-source
  - set protocols bgp network
  - set protocols bgp network-import-check
  - set protocols bgp peer-group
  - set protocols bgp redistribute
  - set protocols bgp route-map delay-timer
  - set protocols bgp router-id
  - set protocols bgp table-map
  - set protocols bgp timers
  - set protocols bgp update-delay

    - set protocols bgp ebgp-requires-policy
    - set protocols bgp neighbor timers delayopen
    - set protocols bgp neighbor maximum-prefix
    - set protocols bgp neighbor maximum-prefix-out
    - set protocols bgp neighbor port
    - set protocols bgp neighbor sender-as-path-loop-detection
    - set protocols bgp fast-external-failover
    - set protocols bgp confederation identifier
    - set protocols bgp confederation peers
    - set protocols bgp dampening
    - set protocols bgp default local-preference
    - set protocols bgp as-notation
    - set protocols bgp neighbor local-as
- OSPFv2 Commands
    - run clear ospf interface
    - run show ospf border-routers
    - run show ospf database
    - run show ospf interface
    - run show ospf neighbor
    - run show ospf route
    - run show ospf summary-address
    - set protocols ospf aggregation timer
    - set protocols ospf area area-type
    - set protocols ospf area filter-list prefix
    - set protocols ospf area no-summary
    - set protocols ospf area range
    - set protocols ospf area virtual-link
    - set protocols ospf area virtual-link authentication
    - set protocols ospf area virtual-link authentication-key
    - set protocols ospf area virtual-link dead-interval
    - set protocols ospf area virtual-link hello-interval
    - set protocols ospf area virtual-link message-digest-key md5
    - set protocols ospf area virtual-link retransmit-interval
    - set protocols ospf area virtual-link transmit-delay
    - set protocols ospf auto-cost reference-bandwidth
    - set protocols ospf compatible rfc1583
    - set protocols ospf default-information originate
    - set protocols ospf default-metric
    - set protocols ospf interface area
    - set protocols ospf interface authentication-key
    - set protocols ospf interface authentication message-digest
    - set protocols ospf interface cost
    - set protocols ospf interface dead-interval
    - set protocols ospf interface hello-interval
    - set protocols ospf interface message-digest-key md5
    - set protocols ospf interface network
    - set protocols ospf interface priority
    - set protocols ospf interface retransmit-interval
    - set protocols ospf interface transmit-delay
    - set protocols ospf log-adjacency-changes
    - set protocols ospf max-metric router-lsa administrative
    - set protocols ospf max-metric router-lsa on-shutdown
    - set protocols ospf max-metric router-lsa on-startup
    - set protocols ospf multi-instance disable
    - set protocols ospf network area
    - set protocols ospf passive-interface
    - set protocols ospf redistribute
    - set protocols ospf redistribute metric-type
    - set protocols ospf redistribute route-map
    - set protocols ospf router-id
    - set protocols ospf summary-address
    - set protocols ospf timers lsa min-arrival
    - set protocols ospf timers throttle spf
    - set protocols ospf traceoption ism
    - set protocols ospf traceoption lsa
    - set protocols ospf traceoption nsm
    - set protocols ospf traceoption packet
    - set protocols ospf traceoption zebra
    - set protocols ospf graceful-restart enable
    - set protocols ospf capability opaque
    - set protocols ospf graceful-restart grace-period

    - set protocols ospf graceful-restart helper enable
    - set protocols ospf graceful-restart helper planned-only
    - set protocols ospf graceful-restart helper strict-lsa-checking
    - set protocols ospf graceful-restart helper supported-grace-time
    - run graceful-restart prepare ospf
    - run show ospf graceful-restart helper
- OSPFv3 Command Reference
    - set protocols ospf6 area
    - set protocols ospf6 area range
    - set protocols ospf6 area stub
    - set protocols ospf6 area stub no-summary
    - set protocols ospf6 auto-cost reference-bandwidth
    - set protocols ospf6 distance
    - set protocols ospf6 distance-ospf6
    - set protocols ospf6 interface area
    - set protocols ospf6 interface cost
    - set protocols ospf6 interface dead-interval
    - set protocols ospf6 interface hello-interval
    - set protocols ospf6 interface ifmtu
    - set protocols ospf6 interface mtu-ignore
    - set protocols ospf6 interface network
    - set protocols ospf6 interface passive
    - set protocols ospf6 interface priority
    - set protocols ospf6 interface retransmit-interval
    - set protocols ospf6 interface transmit-delay
    - set protocols ospf6 log-adjacency-changes
    - set protocols ospf6 redistribute
    - set protocols ospf6 router-id
    - set protocols ospf6 stub-router administrative
    - set protocols ospf6 timers lsa min-arrival
    - set protocols ospf6 timers throttle spf
    - set protocols ospf6 traceoption
    - set protocols ospf6 traceoption border-routers
    - set protocols ospf6 traceoption lsa
    - set protocols ospf6 traceoption message
    - set protocols ospf6 traceoption neighbor
    - set protocols ospf6 traceoption route
    - set protocols ospf6 traceoption spf
    - set protocols ospf6 traceoption zebra
    - set protocols ospf6 graceful-restart enable
    - set protocols ospf6 capability opaque
    - set protocols ospf6 graceful-restart grace-period
    - set protocols ospf6 graceful-restart helper enable
    - set protocols ospf6 graceful-restart helper planned-only
    - set protocols ospf6 graceful-restart helper lsa-checking-disable
    - set protocols ospf6 graceful-restart helper supported-grace-time
    - run graceful-restart prepare ospf6
    - run show ospf6 graceful-restart helper
- Static Route Configuration Commands
    - set protocols static interface-route interface
    - set protocols static mroute
    - set protocols static route
- Route Map Commands
    - run show routing route-map
    - set routing as-path-list
    - set routing large-community-list expanded
    - set routing large-community-list standard
    - set routing prefix-list
    - set routing prefix-list description
    - set routing community-list expanded
    - set routing community-list standard
    - set routing extcommunity-list expanded
    - set routing extcommunity-list standard
    - set routing route-map set-action large-community
    - set routing route-map call
    - set routing route-map description
    - set routing route-map match as-path
    - set routing route-map match community
    - set routing route-map match community-with-exact-match
    - set routing route-map match evpn default-route
    - set routing route-map match evpn route-type

- set routing route-map match evpn vni
- set routing route-map match extcommunity
- set routing route-map matching-policy
- set routing route-map match interface
- set routing route-map match ipv4-addr address
- set routing route-map match ipv4-addr next-hop
- set routing route-map match ipv4-addr route-source
- set routing route-map match ipv6-addr
- set routing route-map match large-community
- set routing route-map match local-preference
- set routing route-map match metric
- set routing route-map match origin
- set routing route-map match peer
- set routing route-map match source-protocol
- set routing route-map match source-vrf
- set routing route-map match tag
- set routing route-map on-match
- set routing route-map set-action aggregator
- set routing route-map set-action as-path exclude
- set routing route-map set-action as-path prepend
- set routing route-map set-action atomic-aggregate
- set routing route-map set-action comm-list-delete
- set routing route-map set-action community
- set routing route-map set-action community-additive
- set routing route-map set-action extcommunity
- set routing route-map set-action extcommunity bandwidth
- set routing route-map set-action extcommunity bandwidth-non-transitive
- set routing route-map set-action ip-next-hop
- set routing route-map set-action ipv4-vpn-next-hop
- set routing route-map set-action ipv6-next-hop
- set routing route-map set-action label-index
- set routing route-map set-action large-comm-list-delete
- set routing route-map set-action local-preference
- set routing route-map set-action metric
- set routing route-map set-action metric-type
- set routing route-map set-action origin
- set routing route-map set-action originator-id
- set routing route-map set-action src
- set routing route-map set-action tag
- set routing route-map set-action weight

- Route Leaking Commands
  - BGP Route Leaking Commands
    - set protocols bgp ipv4-unicast import vrf
    - set protocols bgp ipv6-unicast import vrf
    - set protocols bgp ipv6-unicast import vrf-route-map
    - set protocols bgp vrf ipv4-unicast import vrf
    - set protocols bgp vrf ipv4-unicast import vrf-route-map
    - set protocols bgp vrf ipv6-unicast import vrf
  - Static Route Leaking Commands
    - set protocols static route nexthop-vrf next-hop
    - set protocols static vrf route nexthop-vrf next-hop
- BFD Configuration Commands
  - run show bfd
  - run show bfd counters
  - run show bfd peers
  - set protocols bfd multihop peer local-address
  - set protocols bfd multihop peer local-address detect-multiplier
  - set protocols bfd multihop peer local-address minimum-ttl
  - set protocols bfd multihop peer local-address passive-mode
  - set protocols bfd multihop peer local-address receive-interval
  - set protocols bfd multihop peer local-address shutdown
  - set protocols bfd multihop peer local-address transmit-interval
  - set protocols bfd peer detect-multiplier
  - set protocols bfd peer echo-mode
  - set protocols bfd peer echo receive-interval
  - set protocols bfd peer echo transmit-interval
  - set protocols bfd peer local-address
  - set protocols bfd peer minimum-ttl
  - set protocols bfd peer passive-mode
  - set protocols bfd peer receive-interval
  - set protocols bfd peer shutdown

    - set protocols bfd peer transmit-interval
    - set protocols bfd profile
    - set protocols bfd profile detect-multiplier
    - set protocols bfd profile echo-mode
    - set protocols bfd profile echo receive-interval
    - set protocols bfd profile echo transmit-interval
    - set protocols bfd profile minimum-ttl
    - set protocols bfd profile passive-mode
    - set protocols bfd profile receive-interval
    - set protocols bfd profile shutdown
    - set protocols bfd profile transmit-interval
    - set protocols bgp bfd
    - set protocols ospf6 interface bfd
    - set protocols ospf interface bfd
    - set protocols pim interface bfd
- Policy-Based Routing (PBR) Commands
    - set routing pbr map sequence match destination-ipv4
    - set routing pbr map sequence match source-ipv4
    - set routing pbr map sequence match destination-port
    - set routing pbr map sequence match source-port
    - set routing pbr map sequence match destination-ipv6
    - set routing pbr map sequence match source-ipv6
    - set routing pbr map sequence action nexthop
    - set routing pbr map sequence action dscp
    - set routing pbr map vlan-interface
    - run show pbr map
    - run clear pbr map
- IPv4 Source Guard (IPSG for IPv4) Commands
    - set ip-source-guard binding ip
    - set ip-source-guard enable
    - set ip-source-guard verify
    - set ip-source-guard traceoptions enable
    - run show ip-source-guard binding
- IPv6 Source Guard (IPSG for IPv6) Commands
    - set ipv6-source-guard binding ip
    - set ipv6-source-guard enable
    - set ipv6-source-guard verify
    - set ipv6-source-guard traceoptions enable
    - run show ipv6-source-guard binding
- IS-IS commands
    - set protocols isis area-tag network-entity
    - set protocols isis area-tag is-type
    - set protocols isis area-tag interface
    - set protocols isis area-tag hostname-dynamic
    - set protocols isis area-tag area-password authentication-type
    - set protocols isis area-tag area-password authentication-key
    - set protocols isis area-tag area-password authenticate-snp
    - set protocols isis area-tag domain-password authentication-type
    - set protocols isis area-tag domain-password authentication-key
    - set protocols isis area-tag domain-password authenticate-snp
    - set protocols isis area-tag attached-bit receive-ignore
    - set protocols isis area-tag attached-bit send
    - set protocols isis area-tag log-adjacency-changes
    - set protocols isis area-tag metric-style
    - set protocols isis area-tag set-overload-bit
    - set protocols isis area-tag purge-originator
    - set protocols isis area-tag lsp-mtu
    - set protocols isis area-tag lsp-timers gen-interval
    - set protocols isis area-tag lsp-timers refresh-interval
    - set protocols isis area-tag lsp-timers max-lifetime
    - set protocols isis area-tag spf-interval
    - set protocols isis area-tag spf-delay-ietf init-delay
    - set protocols isis area-tag spf-delay-ietf short-delay
    - set protocols isis area-tag spf-delay-ietf long-delay
    - set protocols isis area-tag spf-delay-ietf holddown
    - set protocols isis area-tag spf-delay-ietf time-to-learn
    - set protocols isis area-tag default-information originate
    - set protocols isis area-tag default-information originate metric
    - set protocols isis area-tag default-information originate route-map
    - set protocols isis area-tag topology ipv6-unicast
    - set protocols isis area-tag interface circuit-type

- set protocols isis area-tag interface csnp-interval
- set protocols isis area-tag interface psnp-interval
- set protocols isis area-tag interface hello-padding
- set protocols isis area-tag interface hello-interval
- set protocols isis area-tag interface hello-multiplier
- set protocols isis area-tag interface metric
- set protocols isis area-tag interface network point-to-point
- set protocols isis area-tag interface passive
- set protocols isis area-tag interface password authentication-type
- set protocols isis area-tag interface password authentication-key
- set protocols isis area-tag interface priority
- set protocols isis area-tag interface three-way-handshake
- set protocols isis area-tag interface bfd
- set protocols isis area-tag interface topology ipv6-unicast
- set protocols isis area-tag redistribute
- set protocols isis traceoption events
- set protocols isis traceoption adj-packets
- set protocols isis traceoption route-events
- set protocols isis traceoption snp-packets
- run show isis summary
- run show isis interface
- run show isis database
- run show isis hostname
- run show isis neighbor
- run show isis route
- run show isis topology

run show neighbors

The **run show neighbors** command is used to view all IPv6 neighbor entries.

Command Syntax

run show neighbors [**vrf** <*vrf-name*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.

Usage Guidelines

When a VRF is specified, only the IPv6 neighbor entries of the specific VRF are displayed.

When no VRF is specified, the result shows only the IPv6 neighbor entries of the default VRF.

Example

- View all IPv6 neighbour entries.

```
admin@Xorplus# run show neighbors
Aging-time(seconds): 1200
Total count        : 1
Address   HW Address     Interface
-----------  -----------------     ---------
2001::1  22:22:22:22:22:22   vlan-2
```

run show route

The **run show route** command shows the information about the IP routing table.

Command Syntax

run show route [**vrf** <*vrf-name*> | <*ip-address*> | **ospf | bgp | static |connected | kernal | ipv4 | ipv6 | summary**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.
<*ip-address*>	Optional. Specifies a destination IP address.

Usage Guidelines

When a VRF is specified, only the routing table information of the specific VRF is displayed.

When no VRF is specified, the result shows only the routing table information of the default VRF.

Example

- View the information about the IP address 40.92.0.0/24.

```
admin@Xorplus# run show route 40.92.0.0/24
RIB entry for 40.92.0.0/24
==========================
Routing entry for 40.92.0.0/24
  Known via "ospf", distance 110, metric 10
  Last update 00:43:58 ago
    directly connected, vlan4092, weight 1

Routing entry for 40.92.0.0/24
  Known via "connected", distance 0, metric 0, best
  Last update 00:44:43 ago
  * directly connected, vlan4092


FIB entry for 40.92.0.0/24
==========================
40.92.0.0/24 dev vlan4092 proto kernel scope link src 40.92.0.1
```

- View the information about the IP routing table of OSPF protocol.

```
admin@Xorplus# run show route ospf
RIB entry for ospf
==================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 1.1.1.1/32 [110/10] via 40.93.0.2, vlan4093, weight 1, 03:01:16
O>* 2.2.2.2/32 [110/10] via 40.94.0.2, vlan4094, weight 1, 00:00:45
O   3.3.3.3/32 [110/0] is directly connected, lo, weight 1, 05:55:08
O>* 4.4.4.4/32 [110/10] via 40.92.0.2, vlan4092, weight 1, 00:47:26
O>* 40.40.0.0/24 [110/30] via 40.92.0.2, vlan4092, weight 1, 00:00:45
  *                       via 40.94.0.2, vlan4094, weight 1, 00:00:45
O   40.92.0.0/24 [110/10] is directly connected, vlan4092, weight 1, 00:47:26
O   40.93.0.0/24 [110/10] is directly connected, vlan4093, weight 1, 03:06:18
```

```
O   40.94.0.0/24 [110/10] is directly connected, vlan4094, weight 1, 00:01:38
```

- View the information about the IP routing table of the default VRF.

```
admin@Xorplus# run show route
show ip route
=============
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K>* 0.0.0.0/0 [0/0] via 10.10.51.1, eth0, 05:48:10
O>* 1.1.1.1/32 [110/10] via 40.93.0.2, vlan4093, weight 1, 02:54:17
O>* 2.2.2.2/32 [110/10] via 40.94.0.2, vlan4094, weight 1, 05:46:52
O   3.3.3.3/32 [110/0] is directly connected, lo, weight 1, 05:48:09
C>* 3.3.3.3/32 is directly connected, lo, 05:48:10
O>* 4.4.4.4/32 [110/10] via 40.92.0.2, vlan4092, weight 1, 00:40:27
C>* 10.10.51.0/24 is directly connected, eth0, 05:48:10



show ipv6 route
===============
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

C * fe80::/64 is directly connected, vlan4092, 00:41:11
C * fe80::/64 is directly connected, vlan4093, 02:59:17
C * fe80::/64 is directly connected, vlan4094, 05:47:4
```

run show route forward-host

The **run show route forward-host** command shows the information about the host hardware forwarding table.

Command Syntax

run show route [**vrf** <*vrf-name*>] **forward-host brief**

run show route [**vrf** <*vrf-name*>] **forward-host ipv4** <*ipv4-address* | **all**>

run show route [**vrf** <*vrf-name*>] **forward-host ipv6** <*ipv6-address* | **all**>

Parameter

Parameter	Description
brief	Displays statistics information about host routes in the IP routing table.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.
ipv4 <*ipv4-address* | **all**>	Specifies an IPv4 address to view the host hardware forwarding table information of a specific IPv4 host, or **all** to view the host hardware forwarding table information of all IPv4 hosts.
ipv6 <*ipv6-address* | **all**>	Specifies an IPv6 address to view the host hardware forwarding table information of a specific IPv6 host, or **all** to view the host hardware forwarding table information of all IPv6 hosts.

Usage Guidelines

When a VRF is specified, only the host hardware forwarding table information of the specific VRF is displayed.

When no VRF is specified, the result shows only the host hardware forwarding table information of the default VRF.

Example

- View the host hardware forwarding table information of all IPv4 hosts.

```
admin@Xorplus# run show route forward-host ipv4 all
Address        HWaddress        Port
---------------   -----------------       ---------
20.20.20.3     70:72:CF:9D:6F:FB   ae3
Total host count:1
```

run show route forward-route

The **run show route forward-route** command is used to view the hardware route forwarding table information.

Command Syntax

run show route [**vrf** <*vrf-name*>] **forward-route brief**

run show route [**vrf** <*vrf-name*>] **forward-route ipv4** {<*IP4Net*>| **all**}

run show route [**vrf** <*vrf-name*>] **forward-route ipv6** {<*IP6Net*>| **all**}

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.
brief	Displays statistics information about routes in the IP routing table.
ipv4 {<*IP4Net*>| **all**}	Specifies an IPv4 network segment address to view the hardware route forwarding table information of a specific IPv4 network segment, or **all** to view the hardware route forwarding table information of all IPv4 network segment.
ipv6 {<*IP6Net*>| **all**}	Specifies an IPv6 network segment address to view the hardware route forwarding table information of a specific IPv6 network segment, or **all** to view the hardware route forwarding table information of all IPv6 network segment.

Usage Guidelines

When a VRF is specified, only the hardware route forwarding table information of the specific VRF is displayed.

When no VRF is specified, the result shows only the hardware route forwarding table information of the default VRF.

Example

- View the hardware route forwarding table information.

```
admin@Xorplus# run show route forward-route ipv4 all
Destination       NextHopMac        Port
---------------      -----------------       ---------
20.20.20.0/24    00:18:23:30:DD:53   connected
Total route count:1
```

- If IP routing function is disabled, the command result shows "**Ip routing is disable**".

```
admin@XorPlus# run show route forward-route ipv4 all
Ip routing is disable
```

run show vrf

The **run show vrf** command is used to view the binding information between the VRFs and the Layer 3 interfaces.

Command Syntax

run show vrf

Parameter

None.

Example

- View the binding information between the VRFs and the Layer 3 interfaces.

```
admin@Xorplus# run show vrf
Vrf          Description       Interfaces
----------   ---------------   -------------------------
vrf1                           vlan1,vlan2
vrf10                          vlan19,vlan20
vrf100                         vlan199,vlan200
vrf101                         vlan201,vlan202
vrf200                         r1.1,r2
```

set ip vrf

The **set ip vrf** command creates a VRF.

Command Syntax

set ip vrf <*vrf-name*> [**description** <*string*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies a VRF name. The value is a string of 1 to 15 case-sensitive characters; spaces are not supported. Note: • Keywords mgmt-vrf, default, vlan.1, ..., vlan.4094, eth0 and eth1 cannot be configured as a VRF name. • A switch supports a maximum of 128 VRFs.
description <*string*>	Optional. Add description information for the VRF. The value is a string.

Example

- Create a VRF vrf1.

```
admin@Xorplus# set ip vrf vrf1 description east
admin@Xorplus# commit
```

set ip routing enable

The **set ip routing enable** command configures whether to enable or disable IP routing function.

NOTE:

- Layer 3 packets cannot be forwarded normally if IP routing function is disabled.
- If the following commit failed message appears when you enable IP routing, the Enterprise License is not installed, and you need to purchase and install the Enterprise License before the L3 feature can be used properly.

```
admin@Xorplus# set ip routing enable true
admin@Xorplus# commit
Command failed: L3 feature is not covered by the installed license key.
Commit failed.
```

Command Syntax

set ip routing enable [**true | false**]

Parameter

Parameter	Description
enable [**true	false**]	Configures whether to enable or disable IP routing function. The value is **true** or **false**. **true**: enables the IP routing function. **false**: disables the IP routing function. The default value is **false**.

Example

- Disable the IP routing function.

```
admin@Xorplus# set ip routing enable false
admin@Xorplus# commit
```

- Enable the IP routing function.

```
admin@Xorplus# set ip routing enable true
admin@Xorplus# commit
```

set system management-vrf enable

The **set system management-vrf enable** command is used to enable or disable management VRF.

Command Syntax

set system management-vrf enable <true | false>

Parameter

Parameter	Description
enable <**true** | **false**>	Enables or disables management VRF. The value could be **true** or **false**. • **true**: enables management VRF. • **false**: disables management VRF. By default, management VRF is disabled.

Usage Guidelines

By default, PICOS starts up with only default VRF, management VRF function is disabled. To enhance the security of the management network, and prevent attacks by illegal users, users can use this command to enable management VRF. Once management VRF is enabled, a VRF with fixed name **mgmt-vrf** is created by the system, Eth0 management interface is automatically moved from the default VRF to the management VRF.

Management VRF is dedicated to transmit the management traffic. Other VRFs are used to transmit the data traffic, thus separating the management traffic from the data traffic effectively.

Example

- Enable management VRF.

```
admin@Xorplus# set system management-vrf enable true
admin@Xorplus# commit
```

BGP Commands

- run show bgp
- run show bgp neighbor
- run show bgp route
- run show bgp unicast neighbor graceful-restart
- set protocols bgp aggregate-address
- set protocols bgp always-compare-med
- set protocols bgp bestpath as-path type multipath-relax
- set protocols bgp bestpath bandwidth
- set protocols bgp bestpath compare-routerid
- set protocols bgp bestpath med missing-as-worst
- set protocols bgp cluster-id
- set protocols bgp graceful-shutdown
- set protocols bgp listen
- set protocols bgp local-as
- set protocols bgp max-med
- set protocols bgp multipath maximum-paths
- set protocols bgp neighbor activate
- set protocols bgp neighbor addpath-tx-all-paths
- set protocols bgp neighbor addpath-tx-bestpath-per-as
- set protocols bgp neighbor advertisement-interval
- set protocols bgp neighbor allowas-in
- set protocols bgp neighbor as-override
- set protocols bgp neighbor capability extended-nexthop
- set protocols bgp neighbor default-originate
- set protocols bgp neighbor description
- set protocols bgp neighbor disable-connected-check
- set protocols bgp neighbor ebgp-multihop
- set protocols bgp neighbor filter-list
- set protocols bgp neighbor next-hop-self
- set protocols bgp neighbor password
- set protocols bgp neighbor peer-group
- set protocols bgp neighbor prefix-list
- set protocols bgp neighbor remote-as
- set protocols bgp neighbor remove-private-as
- set protocols bgp neighbor route-map
- set protocols bgp neighbor route-reflector-client
- set protocols bgp neighbor send-community
- set protocols bgp neighbor shutdown
- set protocols bgp neighbor soft-reconfiguration
- set protocols bgp neighbor timers connect
- set protocols bgp neighbor timers holdtime
- set protocols bgp neighbor timers keepalive
- set protocols bgp neighbor ttl-security hops
- set protocols bgp neighbor update-source
- set protocols bgp network
- set protocols bgp network-import-check
- set protocols bgp peer-group
- set protocols bgp redistribute
- set protocols bgp route-map delay-timer
- set protocols bgp router-id
- set protocols bgp table-map
- set protocols bgp timers
- set protocols bgp update-delay
- set protocols bgp ebgp-requires-policy
- set protocols bgp neighbor timers delayopen
- set protocols bgp neighbor maximum-prefix
- set protocols bgp neighbor maximum-prefix-out
- set protocols bgp neighbor port
- set protocols bgp neighbor sender-as-path-loop-detection
- set protocols bgp fast-external-failover
- set protocols bgp confederation identifier

- set protocols bgp confederation peers
- set protocols bgp dampening
- set protocols bgp default local-preference
- set protocols bgp as-notation
- set protocols bgp neighbor local-as

run show bgp

The **run show bgp** command to displays the BGP routing table.

Command Syntax

run show bgp

Parameter

None.

Example

- View the BGP routing table.

```
admin@Xorplus# run show bgp
show bgp ipv4 unicast
=====================
BGP table version is 2, local router ID is 4.4.4.4, vrf id 0
Default local pref 100, local AS 200
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0/24
                    192.168.20.1             0             100 32768 i

Displayed  1 routes and 1 total paths


show bgp ipv6 unicast
=====================
No BGP prefixes displayed, 0 exist
```

run show bgp neighbor

The **run show bgp neighbor** command displays information about BGP peers.

Command Syntax

run show bgp [**vrf**<*vrf-name*>] **neighbor** [<*ip*> [**advertised-routes | received-routes | routes**]]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>]. If not specified, displays information about BGP peers in the default VRF; If specified, displays information about BGP peers in the specified VRF.
<*ip*>	Optional. Specifies the IP address of a peer. If not specified, it will display information of all the BGP peers.
[**advertised-routes	received-routes	routes**]	Optional. • **advertised-routes:** Displays the routes advertised to a specified peer. • **received-routes:** Displays the routes received from a specified peer. • **route:** Displays all the routes received or advertised to a specified peer.

Example

- View the information about all the BGP peers.

```
admin@Xorplus# run show bgp neighbor
BGP neighbor on vlan20: 192.168.20.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 1.1.1.1, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  Waiting for Peer IPv6 LLA
BGP Connect Retry Timer in Seconds: 120
Read thread: off  Write thread: off  FD used: -1
```

```
BGP neighbor is 192.168.30.2, remote AS 200, local AS 200, internal link
 Administratively shut down
  BGP version 4, remote router ID 3.3.3.3, local router ID 2.2.2.2
  BGP state = Idle
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 600 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
Read thread: off  Write thread: off  FD used: -1

BGP neighbor is 192.168.40.2, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 4.4.4.4, local router ID 2.2.2.2
  BGP state = Active
  Last read 00:15:06, Last write never
  Hold time is 180, keepalive interval is 60 seconds
  Graceful restart information:
    Local GR Mode: Helper*
    Remote GR Mode: NotApplicable
    R bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  0          0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Not part of any update group
  Advertise bestpath per AS via addpath
  Override ASNs in outbound updates if aspath equals remote-as
```

```
  Community attribute sent to this neighbor(all)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset 00:15:06,  No AFI/SAFI activated for peer
  External BGP neighbor may be up to 255 hops away.
BGP Connect Retry Timer in Seconds: 111
Peer Authentication Enabled
Read thread: off  Write thread: off  FD used: -1
```

run show bgp route

The **run show bgp route** command displays BGP route information of a specified route.

Command Syntax

run show bgp route <*ip*>

Parameter

Parameter	Description
<*ip*>	Specifies the IP address. It's in the form of a *ipv4-address* or *ipv6-address* or *ip-address/prefix-lenghth*.

Example

- View the BGP route information of 192.168.10.0/24.

```
admin@Xorplus# run show bgp route 192.168.10.0/24
BGP routing table entry for 192.168.10.0/24
Paths: (1 available, best #1, table default)
  Advertised to non peer-group peers:
  192.168.50.2
  200
    192.168.10.0 from 192.168.20.1 (2.2.2.2)
      Origin IGP, metric 0, valid, external, best (First path received)
      Last update: Wed Apr  7 16:13:35 2021
```

run show bgp unicast neighbor graceful-restart

The **run show bgp unicast neighbor graceful-restart** command displays information about BGP graceful restart in the default VRF. To show information about BGP graceful restart in user-defined VRF, users can run command "**run show bgp vrf** <*vrf-name*> **neighbor** <*ip*>".

Command Syntax

run show bgp <**ipv4|ipv6**> **unicast neighbor** <*ip*> **graceful-restart**

Parameter

Parameter	Description
<**ipv4|ipv6**>	Specifies the IP type, the value could be **ipv4** or **ipv6**.
neighbor <*ip*>	Specifies the IP address of a peer. If not specified, it will display information of all the BGP peers.

Example

- View the information about BGP graceful restart.

```
admin@Xorplus# run show bgp ipv4 unicast neighbor 1.1.1.1 graceful-restart
Codes: GR - Graceful Restart, * -  Inheriting Global GR Config,
       Restart - GR Mode-Restarting, Helper - GR Mode-Helper,
       Disable - GR Mode-Disable.

Global BGP GR Mode :  Restart

BGP neighbor is 1.1.1.1
    Local GR Mode: Helper
    Remote GR Mode: NotApplicable
    R bit: False
    N bit: False
    Timers:
      Configured Restart Time(sec): 120
      Received Restart Time(sec): 0
```

set protocols bgp aggregate-address

The **set protocols bgp aggregate-address as-set** command creates an aggregate address entry in IPv4 or IPv6 format in the BGP routing table.
The **delete protocols bgp aggregate-address as-set** command removes the specified aggregate address entry.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} aggregate-address** <*ipaddress/prefixlen*> **[as-set | summary-only]**

delete protocols bgp [**vrf** <*vrf-name*>]**{ipv4-unicast|ipv6-unicast} aggregate-address** <*ipaddress/prefixlen*> **[as-set | summary-only]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Required. Specifies the IP address family type.
aggregate-address <*ipaddress/prefixlen*>	• *ipaddress* specifies an aggregate address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128. • *ipaddress* specifies an aggregate address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
as-set	Optional. The AS_PATH attribute advertised for this route will contain an AS_SET consisting of all AS numbers contained in all paths that are being summarized.
summary-only	Optional. Creates the aggregate route but also suppresses advertisements of more-specific routes to all neighbors. This parameter can be used only for IPv6 address family type.

Example
• This example creates an aggregate address entry in the BGP routing table.

```
admin@XorPlus# set protocols bgp ipv4-unicast aggregate-address 10.0.0.0/8
admin@XorPlus# commit
```

set protocols bgp always-compare-med

The **set protocols bgp always-compare-med** command enables comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.
The **delete protocols bgp always-compare-med** command sets comparison of MED to the default setting (disabled).

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **always-compare-med**

delete protocols bgp [**vrf** <*vrf-name*>] **always-compare-med**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

- MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.
- During the best-path selection process, MED comparison is done only among paths from the same autonomous system. Use the command bgp always-compare-med to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

Example

• This example enables comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.

```
admin@XorPlus# set protocols bgp always-compare-med
admin@XorPlus# commit
```

set protocols bgp bestpath as-path type multipath-relax

The **set protocols bgp bestpath as-path type multipath-relax** command configures Border Gateway Protocol (BGP) to treat two BGP routes as equal cost even if their AS-paths differ, as long as their AS-path lengths and other relevant attributes are the same. This allows routes with different AS-paths to be programmed into the forwarding table as equal cost multipath routes. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **delete protocols bgp bestpath as-path type multipath-relax** command restores the default behavior which configures BGP to treat two BGP routes as different costs when their AS-paths differ.

Command Syntax

set protocols bgp [***vrf***<*vrf-name*>] **bestpath as-path multipath-relax type [as-set|no-as-set]**

delete protocols bgp [***vrf***<*vrf-name*>] **bestpath as-path multipath-relax type [as-set|no-as-set]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
[as-set|no-as-set]	Optional. Specifies the AS_PATH attribute advertised for this route weather contain or not contain an AS_SET. • **as-set :** The AS_PATH attribute advertised for this route will contain an AS_SET consisting of all AS numbers. • **no-as-set :** The AS_PATH attribute advertised for this route will not contain an AS_SET.

Example
• This example configures Border Gateway Protocol (BGP) to treat two BGP routes as equal cost without considering the AS-paths value.

```
admin@XorPlus# set protocols bgp bestpath as-path multipath-relax
admin@XorPlus# commit
```

set protocols bgp bestpath bandwidth

The **set protocols bgp bestpath bandwidth** command can be used to control link bandwidth processing on the receiver.
The **delete protocols bgp bestpath bandwidth** command disables the link bandwidth controlling processing on the receiver.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **bestpath bandwidth <ignore|skip-missing|default-weight-for-missing>**

delete protocols bgp [***vrf*** <*vrf-name*>] **bestpath bandwidth <ignore|skip-missing|default-weight-for-missing>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
bandwidth <ignore|skip-missing|default-weight-for-missing>	Specifies link bandwidth controlling processing on the receiver. The different options imply behavior as follows: • ignore: Ignore link bandwidth completely for route installation (i.e., do regular ECMP, not weighted) • skip-missing: Skip paths without link bandwidth and do UCMP among the others (if at least some paths have link-bandwidth) • default-weight-for-missing: Assign a low default weight (value 1) to paths not having link bandwidth

Usage Guidelines

This configuration is per BGP instance similar to other BGP route-selection controls; it operates on both IPv4-unicast and IPv6-unicast routes in that instance. In an EVPN network, this configuration (if required) should be implemented in the tenant VRF and is again applicable for IPv4-unicast and IPv6-unicast, including the ones sourced from EVPN type-5 routes.

Example

• This example is a FRR configuration on a receiver to skip paths without link bandwidth.

```
admin@XorPlus# set protocols bgp bestpath bandwidth skip-missing
admin@XorPlus# commit
```

set protocols bgp bestpath compare-routerid

The **set protocols bgp bestpath compare-routerid** command configures a BGP routing process to compare identical routes received from different external peers during the best path selection process and selects the route with the lowest router ID as the best path. Defaults to disabled.
Any changes in BGP configuration are applied by restarting the current BGP sessions in the VRFs.
The **delete protocols bgp bestpath compare-routerid** command returns the BGP routing process to the default operation. By default, BGP selects the route that was received first when two routes with identical attributes are received.

Command Syntax

set protocols bgp [***vrf***<*vrf-name*>] **bestpath compare-routerid**

delete protocols bgp [***vrf***<*vrf-name*>] **bestpath compare-routerid**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example configures a BGP routing process to compare identical routes received from different external peers during the best path selection process and selects the route with the lowest router ID as the best path.

```
admin@XorPlus# set protocols bgp bestpath compare-routerid
admin@XorPlus# commit
```

set protocols bgp bestpath med missing-as-worst

The **set protocols bgp bestpath med missing-as-worst** command configures a BGP routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute. The path without a MED value is the least desirable path. Any changes in BGP configuration are applied by restarting the current BGP sessions in the VRFs.

The **delete protocols bgp bestpath med missing-as-worst** command restores default behavior. The default behavior assigns a value of 0 to the missing MED.

Command Syntax

set protocols bgp [***vrf*** <*vrf-name*>] **bestpath med missing-as-worst**

delete protocols bgp [***vrf*** <*vrf-name*>] **bestpath med missing-as-worst**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example configures a BGP routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute.

```
admin@XorPlus# set protocols bgp bestpath med missing-as-worst
admin@XorPlus# commit
```

set protocols bgp cluster-id

The **set protocols bgp cluster-id** command specifies the cluster ID when the BGP router is used as a route-reflector. The cluster ID default is the router ID. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **delete protocols bgp cluster-id**command sets the cluster ID to the default value, which is the router ID.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **cluster-id** <*IPV4-ADDR*>

delete protocol bgp [**vrf** <*vrf-name*>] **cluster-id** <*IPV4-ADDR*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<*IPV4-ADDR*>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100.

Example
• This example specifies the cluster ID when the BGP router is used as a route-reflector.

```
admin@XorPlus# set protocols bgp cluster-id 2.2.2.2
admin@XorPlus# commit
```

set protocols bgp graceful-shutdown

The **set protocols bgp graceful-shutdown** command enable graceful shutdown. To reduce packet loss during planned maintenance of a router or link, you can configure graceful BGP shutdown, which forces traffic to route around the BGP node.
The **delete protocols bgp graceful-shutdown** command disables graceful BGP shutdown.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **graceful-shutdown**

delete protocols bgp [**vrf** <*vrf-name*>] **graceful-shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example enables graceful shutdown.

```
admin@XorPlus# set protocols bgp graceful-shutdown
admin@XorPlus# commit
```

set protocols bgp listen

The **set protocols bgp listen** command configures BGP dynamic neighbors listen parameters.
The **delete protocols bgp listen** command removes the configuration of BGP dynamic neighbors listen parameters.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **listen** [**limit** <*limit-number*>| **range** <*listen-range*> [**peer-group** <*peer-group*>]]

delete protocols bgp [**vrf** <*vrf-name*>] **listen [limit** <*limit-number*>| **range**<*listen-range*> [**peer-group** <*peer-group*>]**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
limit <*limit-number*>	Optional. Specifies the number of dynamic peers. The value is an integer that ranges from 1 to 5000. The default value is 100.
range<*listen-range*>	Optional. Specifies the BGP dynamic neighbors listen range. The value is in the format of <*ipaddress/prefixlen*>. • *ipaddress* specifies an aggregate address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128. • *ipaddress* specifies an aggregate address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. *prefixlen* specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128. When specifying the BGP dynamic neighbors listen range, you can also set the peer group.

Example
• This example limits the number of dynamic peers to 5.

```
admin@XorPlus# set protocols bgp listen limit 5
admin@XorPlus# commit
```

set protocols bgp local-as

Users can set the Autonomous System (AS) number for this domain.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*>
delete protocols bgp [vrf <*vrf-name*> **local-as** <*AS-NUMBER*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
local-as <*AS-NUMBER*>	Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example
• This example sets AS number as 5:

```
admin@XorPlus# set protocols bgp local-as 5
admin@XorPlus# commit
```

set protocols bgp max-med

The **set protocols bgp max-med** command sets that advertise routes with max-med attribute.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **max-med [administrative med** <*AS-NUMBER*>| **on-startup [duration** <*period*> **| med** <*AS-NUMBER*>**]]**
delete protocols bgp [vrf <*vrf-name*> **max-med [administrative med** <*AS-NUMBER*>**| on-startup [duration** <*period*> **| med** <*AS-NUMBER*>**]]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
administrative med <*AS-NUMBER*>	Optional. Specifies a 4-byte AS number in asplain format (z), where z is a number from 0 to 4294967295. Note that this is administratively applied, for an indefinite period.
duration <*period*>	Optional. Specifies the time period for max-med, which will be effective on a startup. The value is an integer, in seconds, that rangs from 5 to 86400 seconds.
med <*AS-NUMBER*>	Optional. Specifies the Max MED value to be used on a startup. The value is an integer that rangs from 0 to 4294967295.

Example
• This example sets advertise routes with max-med attribute, where Max MED value is 120.

```
admin@XorPlus# set protocols bgp max-med administrative med 120
admin@XorPlus# commit
```

set protocols bgp multipath maximum-paths

The **set protocols bgp multipath maximum-paths** command configures the maximum number of paths that BGP adds to the route table for equal-cost multipath (ECMP) load balancing for routes learned from either internal or external BGP. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **delete protocols bgp multipath maximum-paths** command restores the default setting.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **{ipv4-unicast | ipv6-unicast} multipath** {**ibgp | ebgp} maximum-paths** <*MAXPATHS*>

delete protocol bgp [**vrf** <*vrf-name*>] **{ipv4-unicast | ipv6-unicast} multipath** {**ibgp | ebgp}** [**maximum-paths]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast | ipv6-unicast}	Specifies the IPv4 unicast or IPv6 unicast.
{**ibgp | ebgp}**	Specifies the internal or external BGP.
<*MAXPATHS*>	Specifies the maximum number of paths. You can set a value between 1 and 32. 1 disables the BGP multipath option.

Example
• This example changes the maximum number of paths to 12.

```
admin@XorPlus# set protocols bgp ipv4-unicast multipath ibgp maximum-paths 12
admin@XorPlus# commit
```

set protocols bgp neighbor activate

The **set protocols bgp neighbor activate** command enables the address-family capability and exchange of information specific to an address family with a BGP neighbor.
The **delete protocols bgp neighbor activate** command removes the address-family capability and disables the exchange of routes for the specified address-family with the BGP neighbor.

For IPv6 BGP configuration, the following command must be configured to enable the IPv6 address family capability and exchange of information specific to an IPv6 address family with a BGP neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **activate <true | false>**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **activate**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
<true | false>	Enables or disables the address-family capability. The value could be **true** or **false**. • **true**: enables the address-family capability. • **false**: disables the address-family capability.

Example
• This example enables the address-family capability and exchange of information specific to an address family with a BGP neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast activate true
admin@XorPlus# commit
```

set protocols bgp neighbor addpath-tx-all-paths

The **set protocols bgp neighbor addpath-tx-all-paths** command advertises all known paths to a neighbor.
The **delete protocols bgp neighbor addpath-tx-all-paths** command disables the additional path feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-all-paths**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-all-paths**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example advertises all known paths to a neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast addpath-tx-all-paths
admin@XorPlus# commit
```

set protocols bgp neighbor addpath-tx-bestpath-per-as

The **set protocols bgp neighbor addpath-tx-bestpath-per-as** command advertises only the best path learned from each AS to a neighbor.
The **delete protocols bgp neighbor addpath-tx-bestpath-per-as** command disables the additional path feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-bestpath-per-as**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **addpath-tx-bestpath-per-as**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example advertises only the best path learned from each AS to a neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast addpath-tx-bestpath-per-as
admin@XorPlus# commit
```

set protocols bgp neighbor advertisement-interval

The **set protocols bgp neighbor advertisement-interval** command sets the advertisement interval, which defines the length of time between transmission of BGP routing updates.

The **delete protocols bgp neighbor advertisement-interval** command restores the default value. Default values are 30 seconds for external BGP peer and 5 seconds for internal BGP peer.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} advertisement-interval** <*advert-interval*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} advertisement-interval**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
advertisement-interval <*advert-interval*>	Specifies the advertisement interval in seconds. Range: 0 to 600. Default: 30 for external BGP peer and 5 for internal BGP peer.

Example
• This example sets the advertisement interval to 20 seconds.

```
admin@XorPlus# set protocols bgp neighbor 1.1.1.1 advertisement-interval 20
admin@XorPlus# commit
```

set protocols bgp neighbor allowas-in

The **set protocols bgp neighbor allowas-in** command specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP speaker and still be accepted. When this configuration is applied to a peer-group, all the neighbors that are part of the peer-group inherit this setting.
The **delete protocols bgp neighbor allowas-in** command restores the default setting, which is to reject as a loop any route where the path contains the speaker AS number.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **allowas-in {**<*LIMIT*>**|origin}**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **allowas-in {**<*LIMIT*>**|origin}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
allowas-in {<*LIMIT*>**|origin}**	<*LIMIT*>: Specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP. Range: 1 to 10. **origin:** The parameter origin configures BGP to only accept routes originated with the same AS number as the system. This command is only allowed for eBGP peers.

Example
• This example specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP speaker and still be accepted.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast allowas-in 5
admin@XorPlus# commit
```

set protocols bgp neighbor as-override

The **set protocols bgp neighbor as-override** command overrides AS number of the originating router with the local AS number.
The **delete protocols bgp neighbor as-override** command restores the default setting.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **as-override**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **as-override**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines

Usually this configuration is used in PEs (Provider Edge) to replace the incoming customer AS number so the connected CE (Customer Edge) can use the same AS number as the other customer sites. This allows customers of the provider network to use the same AS number across their sites.
This command is only allowed for eBGP peers.

Example

• This example overrides AS number of the originating router with the local AS number.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast as-override
admin@XorPlus# commit
```

set protocols bgp neighbor capability extended-nexthop

The **set protocols bgp neighbor capability extended-nexthop** command enables advertisement of IPv4 prefixes with IPv6 next hops over global IPv6 peerings, adding the extended-nexthop capability to the global IPv6 neighbor statements on each end of the BGP sessions.
The **delete protocols bgp neighbor capability extended-nexthop** command disables advertisement of IPv4 prefixes with IPv6 next hops over global IPv6 peerings.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} capability extended-nexthop**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} capability extended-nexthop**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines

Allow BGP to negotiate the extended-nexthop capability with it's peer. If you are peering over a IPv6 link-local address then this capability is turned on automatically. If you are peering over a IPv6 Global Address then turning on this command will allow BGP to install IPv4 routes with IPv6 nexthops if you do not have IPv4 configured on interfaces.

Example
• This example enables advertisement of IPv4 prefixes with IPv6 next hops over global IPv6 peerings.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 capability extended-nexthop
admin@XorPlus# commit
```

set protocols bgp neighbor default-originate

The **set protocols bgp neighbor default-originate** command enables the local router to send the default route 0.0.0.0 to a neighbor. The neighbor can then use this route to reach the router when all other routes are unavailable.
The **delete protocols bgp neighbor default-originate** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **default-originate [route-map** <*MAP-NAME*>**]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **default-originate [route-map** <*MAP-NAME*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
route-map <*MAP-NAME*>	Optional. Sets the route map to modify the default route attributes.

Example
• This example enables the local router to send the default route 0.0.0.0 to a neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast default-originate
admin@XorPlus# commit
```

set protocols bgp neighbor description

The **set protocols bgp neighbor description** command configures a description for a peer or peer group.

The **delete protocols bgp neighbor description** command deletes the description of a peer or peer group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} description <***description-text***>**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} *description* <***description-text***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
description <*description-text***>**	Specifies a description. The value is a string.

Example

• Configure a description for a peer.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 description Leaf1
admin@XorPlus# commit
```

set protocols bgp neighbor disable-connected-check

The **set protocols bgp neighbor disable-connected-check** command allows peerings between directly connected eBGP peers using loopback addresses. The **delete protocols bgp neighbor disable-connected-check** command doesn't allow peerings between directly connected eBGP peers using loopback addresses.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} disable-connected-check**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} disable-connected-check**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example

• This example allows peerings between directly connected eBGP peers using loopback addresses.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 disable-connected-check
admin@XorPlus# commit
```

set protocols bgp neighbor ebgp-multihop

The **set protocols bgp neighbor ebgp-multihop** command enables BGP to establish a session with external peers residing on networks that are not directly connected. By default, BGP can only establish sessions with external BGP peers that are directly connected. The neighbor connection must be reset using clear bgp to allow this configuration to take effect.

The **delete protocols bgp neighbor ebgp-multihop** command disables the peer ebgp-multihop feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*>**} ebgp-multihop** [**maximum-hop** <*HOP-COUNT*>]

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*>**} ebgp-multihop** [**maximum-hop** <*HOP-COUNT*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
maximum-hop <*HOP-COUNT*>	Optional. Specifies the maximum number of hops to reach the peer. The value is an integer that ranges from 1 to 255.

Example
• This example enables BGP to establish connection with external peers residing on networks that are not directly connected:

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ebgp-multihop maximum-hop 5

admin@XorPlus# commit
```

set protocols bgp neighbor filter-list

The **set protocols bgp neighbor filter-list** command configures an AS Path list to advertise or receive routes from peers.

The **delete protocols bgp neighbor filter-list** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} filter-list** <*as-path-list*>

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} filter-list** <*as-path-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
filter-list <*as-path-list*>	Specifies the AS Path list, which is configured by the command **set routing as-path-list**.
{in|out}	Sets the filter policy to apply to either the received routes from the neighbor (in) or the advertised routes to the neighbor (out).

Example

• This example configures an AS Path list to receive routes from peers.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in filter-list List1
admin@XorPlus# commit
```

set protocols bgp neighbor next-hop-self

The **set protocols bgp neighbor next-hop-self** command configures the router as the next hop for a BGP-speaking neighbor or peer group, and enables BGP to send itself as the next hop for advertised routes.
The **delete protocols bgp neighbor next-hop-self** command resets the peer nexthop-self status to default. The next hop will be generated based on the IP.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **next-hop-self [force]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **next-hop-self [force]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example configures the router as the next hop for a BGP-speaking neighbor or peer group, and enables BGP to send itself as the next hop for advertised routes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast next-hop-self
admin@XorPlus# commit
```

set protocols bgp neighbor password

The **set protocols bgp neighbor password** command enables message digest5 (MD5) authentication on a TCP connection between two BGP neighbors. When the password is applied to a peer-group, all the neighbors that are part of peer-group inherit the configured
setting. The neighbor connection must be reset using clear ip bgp to allow this configuration to take effect.

The **delete protocols bgp neighbor password** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} password** <*text-password*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} password**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
password <*text-password*>	Specifies the txt password.

Example
• This example enables message digest5 (MD5) authentication on a TCP connection between two BGP neighbors.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 password picos12345
admin@XorPlus# commit
```

set protocols bgp neighbor peer-group

The **set protocols bgp neighbor peer-group** command adds a peer to a peer group.
The **delete protocols bgp neighbor peer-group** command removes a peer to a peer group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*> | **interface** <*interface*>**} peer-group** <*peergroup*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*> | **interface** <*interface*>**} peer-group** <*peergroup*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
peer-group <*peergroup*>	Specifies a peer group name. The value is a string.

Usage Guidelines

Instead of specifying properties of each individual peer, you can define one or more peer groups and associate all the attributes common to that peer session to a peer group. A peer needs to be attached to a peer group only once, when it then inherits all address families activated for that peer group.

Note:

If the peer you want to add to a group already exists in the BGP configuration, delete it first, than add it to the peer group.

Example

• This example adds two peers to a peer group **leaf1**.

```
admin@XorPlus# set protocols bgp neighbor 10.10.0.1 peer-group leaf1
admin@XorPlus# set protocols bgp neighbor 10.10.0.12 peer-group leaf1
admin@XorPlus# commit
```

set protocols bgp neighbor prefix-list

The **set protocols bgp neighbor prefix-list** command configures an IPv4 or IPv6 prefix list to advertise or receive routes from peers.

The **delete protocols bgp neighbor prefix-list** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} prefix-list** <*prefix-list*>

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} prefix-list** <*prefix-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4 or IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
prefix-list <*prefix-list*>	Specifies the IPv4 or IPv6 prefix list.
{in|out}	Sets the filter policy to apply to either the received routes from the neighbor (in) or the advertised routes to the neighbor (out).

Example

• This example configures an IPv4 prefix list to receive routes from peers.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in prefix-list List1
admin@XorPlus# commit
```

set protocols bgp neighbor remote-as

The **set protocols bgp neighbor remote-as** command creates a peer, initiates the connection to the peer, and adds an entry to the BGP neighbor table. Specifies a neighbor with an autonomous system (AS) number that identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external. By default, neighbors that are defined using this command, exchange only unicast address prefixes.
The **delete protocols bgp neighbor remote-as** command disables the peer session and deletes the peer information.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} remote-as {**<*as-number*>**|external|internal}**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} remote-as {**<*as-number*>**|external|internal}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
remote-as {<*as-number*>**|external|internal}**	<*as-number*>: Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535. **external**: Create a peer as you would when you specify an ASN, except that if the peers ASN is the same as mine as specified under this command the connection will be denied. **internal**: Create a peer as you would when you specify an ASN, except that if the peers ASN is different than mine as specified under tis command the connection will be denied.

Example
• This example specifies a neighbor with an autonomous system (AS) number.

```
admin@XorPlus# set protocols bgp neighbor 10.10.0.1 remote-as 100
admin@XorPlus# commit
```

set protocols bgp neighbor remove-private-as

The **set protocols bgp neighbor remove-private-as** command removes private ASNs from routes sent to the neighbor.

The **delete protocols bgp neighbor remove-private-as** command allows the private-AS number to be carried in BGP update message.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **remove-private-as [all] [replace-as]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} {ipv4 unicast|ipv4 labeled-unicast|ipv6 unicast|ipv6 labeled-unicast} remove-private-as [all] [replace-as]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
[all]	Optional. Apply to all AS numbers.
[replace-as]	Optional. Replaces the private ASNs with your public ASN.

Usage Guidelines

If you use private ASNs in the data center, any routes you send out to the internet contain your private ASNs. You can remove all the private ASNs from routes to a specific neighbor.

Example

• This example removes private ASNs from routes sent to the neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast remove-private-as
admin@XorPlus# commit
```

set protocols bgp neighbor route-map

The **set protocols bgp neighbor route-map** command applies a route map to incoming or outgoing routes. It configures the route map for modifying the default attributes of the route.
The **delete protocols bgp neighbor route-map** command removes a route map.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} route-map** <*route-map*>

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **{in|out} route-map** <*route-map*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
route-map <*route-map*>	Specifies the name of the route map.
{in|out}	Sets the route map policy to apply to either the received routes from the neighbor (in) or the advertised routes to the neighbor (out).

Example
• This example applies a route map to the incoming routes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast in route-map map1
admin@XorPlus# commit
```

set protocols bgp neighbor route-reflector-client

The **set protocols bgp neighbor route-reflector-client** command configures the router as a BGP route reflector and the specified peer as its client.
The **delete protocols bgp neighbor route-reflector-client** command disables this function.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **route-reflector-client**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **route-reflector-client**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example configures the router as a BGP route reflector and the specified peer as its client.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast route-reflector-client
admin@XorPlus# commit
```

set protocols bgp neighbor send-community

The **set protocols bgp neighbor send-community** command enables community and/or extended community exchange with the specified neighbor. When this command is configured for the peer-group, then all the neighbors that are part of peer-group will send the community values to the peers.
The **delete protocols bgp neighbor send-community** command will not allow the neighbor to send community values to the specific neighbors that are part of peer-group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **send-community type [both|extended|standard|large|all]**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **send-community type [both|extended|standard|large|all]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
[both|extended|standard|large|all]	Optional. The parameters **standard**, **large** and **extended** send only the respective community numbers. **all**: both standard and extended communities will be sent to the neighbor.

Example
• This example allows community values to be sent to a specific neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast send-community type both
admin@XorPlus# commit
```

set protocols bgp neighbor shutdown

The **set protocols bgp neighbor shutdown** command disables the peer session, terminates any active session for the specified neighbor or peer group, and removes all associated routing information. This action can cause the sudden termination of many peering sessions.

The **delete protocols bgp neighbor shutdown** command enables the peer session for the specified neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} shutdown**

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines
Sessions are gracefully shut down when graceful-shutdown is enabled. Use the set protocols bgp graceful-shutdown command to enable graceful-shutdown. If graceful-shutdown is configured without delay or localpreference, the default values are used.

Example
• This example disables the peer session for the specified neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 shutdown
admin@XorPlus# commit
```

set protocols bgp neighbor soft-reconfiguration

The **set protocols bgp neighbor soft-reconfiguration** command enables you to generate inbound updates from a neighbor and change and activate BGP policies without clearing the BGP session. Changes in BGP policies require the BGP session to be cleared which can have a large negative impact on network operations. The **delete protocols bgp neighbor soft-reconfiguration** command disables this setting.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **soft-reconfiguration inbound**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**}** {**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**} **soft-reconfiguration inbound**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{**ipv4-unicast|ipv4-labeled-unicast|ipv6-unicast|ipv6-labeled-unicast**}	Specifies the type of the address family.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Usage Guidelines

- To perform inbound soft reconfiguration, the BGP speaker must store all received route updates, regardless of the current inbound policy.
- When inbound soft reconfiguration is enabled, the stored updates are processed by the new policy configuration to create new inbound updates.

Example

• This example enables to generate inbound updates from a neighbor and change and activate BGP policies without clearing the BGP session.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast soft-reconfiguration inbound
admin@XorPlus# commit
```

set protocols bgp neighbor timers connect

By default, the BGP process attempts to connect to a peer after a failure (or on startup) every 10 seconds. You can change this value to suit your needs.

The **set protocols bgp neighbor timers connect** command sets the reconnect value.
The **delete protocols bgp neighbor timers connect** command removes the configurations.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers connect** <*timers*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers connect**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
timers connect <*timers*>	Specifies the reconnect timer value for the neighbor. Default: 10 seconds. Range: 1-65535.

Example
• This example sets the reconnect value to 30 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers connect 30
admin@XorPlus# commit
```

set protocols bgp neighbor timers holdtime

The **set protocols bgp neighbor timers connect holdtime** command sets the hold time for a BGP peer.
The **delete protocols bgp neighbor timers connect holdtime** command removes the configurations.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers holdtime** <*hold time*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers holdtime**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
<*hold time*>	Specifies the hold time. Default: 180 seconds. Range: 0-65535.

Usage Guidelines

By default, BGP exchanges periodic keepalive messages to measure and ensure that a peer is still alive and functioning. If a keepalive or update message is not received from the peer within the hold time, the peer is declared down and all routes received by this peer are withdrawn from the local BGP table. By default, the keepalive interval is set to 60 seconds and the hold time is set to 180 seconds. To decrease CPU load, especially in the presence of a lot of neighbors, you can increase the values of these timers or disable the exchange of keepalives entirely. When manually configuring new values, the keepalive interval can be less than or equal to one third of the hold time, but cannot be less than 1 second. Setting the keepalive and hold time values to 0 disables the exchange of keepalives.

Example

• This example set the hold time to 200 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers holdtime 200
admin@XorPlus# commit
```

set protocols bgp neighbor timers keepalive

The **set protocols bgp neighbor timers connect keepalive** command sets the keepalive interval for a BGP peer.
The **delete protocols bgp neighbor timers connect keepalive** command removes the configurations.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers keepalive** <*keepalive interval*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} timers keepalive**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
keepalive <*keepalive interval*>	Specifies the keepalive interval value for the neighbor. Default: 60 seconds. Range: 0-65535.

Usage Guidelines

By default, BGP exchanges periodic keepalive messages to measure and ensure that a peer is still alive and functioning. If a keepalive or update message is not received from the peer within the hold time, the peer is declared down and all routes received by this peer are withdrawn from the local BGP table. By default, the keepalive interval is set to 60 seconds and the hold time is set to 180 seconds. To decrease CPU load, especially in the presence of a lot of neighbors, you can increase the values of these timers or disable the exchange of keepalives entirely. When manually configuring new values, the keepalive interval can be less than or equal to one third of the hold time, but cannot be less than 1 second. Setting the keepalive and hold time values to 0 disables the exchange of keepalives.

Example

• This example set the keepalive interval to 80 seconds.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 timers keepalive 80
admin@XorPlus# commit
```

set protocols bgp neighbor ttl-security hops

The **set protocols bgp neighbor ttl-security hops** command enables BGP to establish connection with external peers residing on networks that are not directly connected. By enabling this feature, the received TTL from a BGP peer is compared with the difference "255 - hop-count". BGP messages coming with a TTL less than this value are not accepted. BGP peering will not be established if the TTL in the session establishment is received with a lower value. Also, by enabling this feature the router will send BGP packets with TTL value of 255 to the neighbor. For a neighbor, either TTL security or ebgp-multihop can be configured, not both together. If there are multiple paths to reach the node, then the hop count should be configured considering the longest route.

The **delete protocols bgp neighbor ttl-security hops** command disables the peer ttl-security-hop feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} ttl-security hops** <*HOP-COUNT*>

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} ttl-security hops** <*HOP-COUNT*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
ttl-security hops <*HOP-COUNT*>	Specifies the hop count to reach the neighbor for the eBGP session. Range: 1-254.

Example
• This example enables the peer ttl-security-hop feature.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ttl-security hops 10
admin@XorPlus# commit
```

set protocols bgp neighbor update-source

The **set protocols bgp neighbor update-source** command specifies the source address to reach the neighbor. An iBGP connection can occur as long as there is a TCP/IP path between the routers. If multiple paths exist between the iBGP routers, using a loopback interface as the neighbor address can add stability to the network. With this command, stability can be achieved by providing the loopback interface address as the source address of the TCP/IP session.

The **delete protocols bgp neighbor update-source** command negates the route updates of the neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} update-source** {<*IPv4*>|<*IPv6*> |<*interface-source*>}

delete protocols bgp [**vrf** <*vrf-name*>] {**neighbor** <*ip*>| **peer-group** <*peer-group*> | **interface** <*interface*>**} update-source**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
update-source {<*IPv4*>|<*IPv6*> | <*interface-source*>}	Specifies the source address or source interface. • <*IPV4*>: Specifies an interface by IPv4 address. • <*IPV6*>: Specifies an interface by IPv6 address. • <*interface-source*>: Specifies a source interface name.

Example
• This example specifies the source address to reach the neighbor.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 update-source 10.10.192.1
admin@XorPlus# commit
```

set protocols bgp network

The **set protocols bgp network** command specifies the IPv4/IPv6 networks to be advertised by the Border Gateway Protocol (BGP) routing processes.
The **delete protocols bgp network** command removes an entry from the routing table.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} network <***ip-address/prefixlen*> **[label-index**<*label-index*>|**route-map** <*ROUTE-MAP-NAME*>**]**

delete protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} network** <*ip-address/prefixlen*> **[label-index**<*label-index*>|**route-map** <*ROUTE-MAP-NAME*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Required. Specifies the IP address family type.
<*ip-address/prefixlen*>	Specifies the IPv4/IPv6 network with mask. For example: 1.1.1.0/24
label-index <*label-index*>	Optional parameter. Specifies a route label.
route-map <*ROUTE-MAP-NAME*>	Optional parameter. Specifies a route map to apply to the prefixes advertised by this specific network statement.

Usage Guidelines
• This command is used to advertise prefixes currently installed in the routing table into the BGP table.
• Use the route-map keyword to apply the specified route map to network advertisements. The mask length as configured in the network statement must match the mask length of prefixes in the routing table.

Example
• This example specifies the networks to be advertised by the Border Gateway Protocol (BGP) routing processes.

```
admin@XorPlus# set protocols bgp ipv4-unicast network 11.11.11.0/24
admin@XorPlus# commit
```

set protocols bgp network-import-check

The **set protocols bgp network-import-check** command modifies the behavior of the network statement. If you have this configured the underlying network must exist in the rib.
The **delete protocols bgp network-import-check** command sets that BGP will not check for the networks existence in the rib.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **network-import-check**

delete protocols bgp [**vrf** <*vrf-name*>] **network-import-check**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example modifies the behavior of the network statement.

```
admin@XorPlus# set protocols bgp network-import-check
admin@XorPlus# commit
```

set protocols bgp peer-group

The **set protocols bgp peer-group** command creates a peer group.
The **delete protocols bgp peer-group** command deletes a peer group.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **peer-group** <*peer-group*>

delete protocols bgp [**vrf** <*vrf-name*>] **peer-group** <*peer-group*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer-group <*peer-group*>	Specifies a name of peer group.

Usage Guidelines

Instead of specifying properties of each individual peer, you can define one or more peer groups and associate all the attributes common to that peer session to a peer group. A peer needs to be attached to a peer group only once, when it then inherits all address families activated for that peer group.

Note:

If the peer you want to add to a group already exists in the BGP configuration, delete it first, than add it to the peer group.

Example
• This example creates a peer group.

```
admin@XorPlus# set protocols bgp peer-group leaf1
admin@XorPlus# commit
```

set protocols bgp redistribute

The **set protocols bgp redistribute** command specifies IPv4/IPv6 routes to import into BGP. This command causes routes from the specified protocol to be considered for redistribution into BGP.
The **delete protocols bgp redistribute** command deletes the routes imported into BGP.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} redistribute** {**connected|kernel|ospf|isis|rip|static|table <***table-number***>**} [**metric** <*metric-number*>|**route-map** <*route-map*>]

delete protocols bgp [**vrf** <*vrf-name*>] **{ipv4-unicast|ipv6-unicast} redistribute** {**connected|kernel|ospf|isis|rip|static|table** <*table-number*>} [**metric** <*metric-number*>|**route-map** <*route-map*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Required. Specifies the IP address family type.
redistribute {**connected|kernel|ospf|isis|rip|static|table|table <***table-number***>**}	Redistributes routes to import into BGP. • **connected**: Redistribute connected route to BGP process. • **kernel**: Redistribute kernel route to BGP process. • **ospf**: Redistribute OSPFv2 route to BGP process. • **isis**: Redistribute IS-IS route to BGP process. • **rip**: Redistribute RIP route to BGP process. • **static**: Redistribute static route to BGP process. • **table <***table-number***>**: Redistribute specific route table to BGP process. The value is an integer that ranges from 1 to 65535.
metric <*metric-number*>	Optional. Specifies route metric of the imported routes into BGP. The value is an integer that ranges from 0 to 4294967295.
route-map <*route-map*>	Optional. Specifies the name of the route map.

Example
• This example redistributes OSPF route to BGP process, and the route metric is set to 20.

```
admin@XorPlus# set protocols bgp ipv4-unicast redistribute ospf metric 20
admin@XorPlus# commit
```

set protocols bgp route-map delay-timer

The **set protocols bgp route-map delay-timer** command sets the delay before any route-maps are processed.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **route-map delay-timer** <*delay-timer*>
delete protocols bgp [**vrf** <*vrf-name*> **route-map delay-timer** <*delay-timer*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
delay-timer <*delay-timer*>	Specifies a delay timer. The value is an integer, in second, that ranges from 0 to 600. The default time for this is 5 seconds.

Example
• This example sets the delay before any route-maps are processed.

```
admin@XorPlus# set protocols bgp route-map delay-timer 10
admin@XorPlus# commit
```

set protocols bgp router-id

The **set protocols bgp router-id** command configures a Router ID for the switch.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **router-id** <*router-id*>
delete protocols bgp [**vrf** <*vrf-name*> **router-id** <*router-id*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
router-id <*router-id*>	Specifies a Router ID. It is in dotted decimal notation.

Example
• Configure a Router ID for the switch.

```
admin@XorPlus# set protocols bgp router-id 10.1.1.1
admin@XorPlus# commit
```

set protocols bgp table-map

The **set protocols bgp table-map** command is used to apply a route-map on route updates from BGP to Zebra. All the applicable match operations are allowed, such as match on prefix, next-hop, communities, etc. Set operations for this attach-point are limited to metric and next-hop only. Any operation of this feature does not affect BGPs internal RIB.
Supported for ipv4 and ipv6 address families. It works on multi-paths as well, however, metric setting is based on the best-path only.
The **delete protocols bgp table-map** command disables this feature.

Command Syntax

set protocol bgp [vrf <*text*>**] {ipv4-unicast|ipv6-unicast} table-map** <*route-map-name*>

delete protocol bgp [vrf <*text*>**] {ipv4-unicast|ipv6-unicast} table-map** <*route-map-name*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
{ipv4-unicast|ipv6-unicast}	Specifies the IP address family type.
table-map <*route-map-name*>	Specifies the name of the route map.

Example
• This example applies a route-map on route updates from BGP to Zebra.

```
admin@XorPlus# set protocols bgp ipv4-unicast table-map map1
admin@XorPlus# commit
```

set protocols bgp timers

The **set protocols bgp timers** command sets the timers for all the BGP neighbor.

The **delete protocols bgp timers** command clears the BGP timers.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **timers {holdtime** <*HOLDTIME*>**|keepalive** <*KEEPALIVE*>**}**

delete protocols bgp [**vrf** <*vrf-name*> **timers {holdtime** <*HOLDTIME*>|**keepalive**<*KEEPALIVE*>}

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
keepalive<*KEEPALIVE*>	Specifies the Keep-Alive timer value for the neighbor. Default: 60 seconds. Range: 0-65535.
holdtime <*HOLDTIME*>	Specifies the Hold-timer value. Default: 180 seconds. Range: 0-65535.

Example

• This example sets the keepalive timer for all the BGP neighbor.

```
admin@XorPlus# set protocols bgp timers keepalive 360
admin@XorPlus# commit
```

set protocols bgp update-delay

The **set protocols bgp update-delay** command enable read-only mode by setting the maximum delay timer.

Command Syntax
set protocols bgp [**vrf** <*vrf-name*>] **update-delay {delay** <*maximum delay-timer*>| **establish-wait** <*establish-wait-timer*>}
delete protocols bgp [**vrf** <*vrf-name*> **update-delay delay [delay** <*maximum delay-timer*>| **establish-wait** <*establish-wait-timer*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
delay <*maximum delay-timer*>	Specifies a maximum delay timer. The value is an integer, in second, that ranges from 0 to 3600. The default time for this is 0 seconds, which disables read-only mode.
establish-wait <*establish-wait-timer*>	Optional. Specifies a establish wait timer. The value is an integer, in second, that ranges from 0 to 3600. When specified, it should be less than the maximum delay timer.

Usage Guidelines

To enable read-only mode, you set the maximum delay timer and, optionally, the establish-wait timer. Read-only mode begins as soon as the first peer reaches its established state and the maximum delay timer starts, and continues until either of the following two conditions are met:

- All the configured peers (except the shutdown peers) have sent an explicit EOR (End-Of-RIB) or an implicit EOR. The first keep-alive after BGP reaches the established state is considered an implicit EOR. If you specify the *establish-wait* option, BGP only considers peers that have reached the established state from the moment the maximum delay timer starts until the establish-wait period ends. The minimum set of established peers for which EOR is expected are the peers that are established during the establish-wait window, not necessarily all the configured neighbors.
- The timer reaches the configured maximum delay.

Example
• The following example commands enable read-only mode by setting the maximum delay timer to 300 seconds.

```
admin@XorPlus# set protocols bgp update-delay delay 300
admin@XorPlus# commit
```

set protocols bgp ebgp-requires-policy

The **set protocols bgp ebgp-requires-policy** command determines whether or not EBGP will exchange routes with peers by using a policy.

The **delete protocols bgp ebgp-requires-policy** command restores the default configuration.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **ebgp-requires-policy** <**true | false**>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**true	false**>	Enable or disable ebgp-requires-policy. The value could be **true** or **false**. • **true**: Enable ebgp-requires-policy. • **false**: Disable ebgp-requires-policy. By default, ebgp-requires-policy is enabled.

Usage Guidelines

Consider creating appropriate route maps and using them rather than disabling the policy check, as using policies is a more secure behavior, and can prevent unintended routes from being exchanged. Function ebgp-requires-policy is introduced and enabled by default.

With this command enable, EBGP will not exchange routes with a neighbor unless there is a route map configured on the address family neighbor entry which matches and permits the routes inbound and outbound. That is, without the incoming filter, no routes will be accepted; without the outgoing filter, no routes will be announced.

NOTE:

- If you do not want to control the route exchanging via use BGP policies, you need to disable this feature manually, or the route cannot be correctly exchanged.
- When ebgp-requires-policy is enabled but the incoming or outgoing filter is missing, the route cannot be correctly updated, additionally a **run show bgp neighbor** command would indicate in the *For address family*: block that:

```
admin@Xorplus# run show bgp neighbor
...
For address family: IPv4 Unicast
  Update group 1, subgroup 1
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  Inbound updates discarded due to missing policy
  Outbound updates discarded due to missing policy
  0 accepted prefixes
...
For address family: IPv6 Unicast
  Update group 2, subgroup 2
  Packet Queue length 0
  Community attribute sent to this neighbor(all)
  Inbound updates discarded due to missing policy
  Outbound updates discarded due to missing policy
  0 accepted prefixes
```

Example

- Configure a BGP route policy "rm1" and enable ebgp-requires-policy to filter the incoming routes by using this policy.

```
admin@Xorplus# set routing prefix-list ipv4-family plist1 permit prefix 13.13.13.0/24
admin@Xorplus# set routing route-map rm1 order 1 matching-policy permit
admin@Xorplus# set routing route-map rm1 order 1 match ipv4-addr address prefix-list plist1
admin@Xorplus# set protocols bgp neighbor 192.168.170.1 ipv4-unicast in route-map rm1
admin@Xorplus# set protocols bgp ebgp-requires-policy true
```

```
admin@Xorplus# commit
```

set protocols bgp neighbor timers delayopen

The **set protocols bgp neighbor timers delayopen** command configures the timer to delay sending an OPEN message on a BGP connection. The delay allows the remote BGP Peer time to send the first OPEN message.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*>|**interface** <*interface*>**} timers delayopen** <*delayopen-timer*>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the BGP.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an interface for BGP connection.
delayopen <*delayopen-timer*>	Specifies the time period to delay sending an OPEN message. The value is an integer, in seconds, that ranges from 1 to 240.

Example

- Configure the timer to delay sending an OPEN message on a BGP connection.

```
admin@Xorplus# set protocols bgp neighbor 192.168.170.2 timers delayopen 100
admin@Xorplus# commit
```

set protocols bgp neighbor maximum-prefix

The **set protocols bgp neighbor maximum-prefix** command sets a maximum number of prefixes we can receive from a given neighbor. If this number is exceeded, the BGP session will be destroyed.
The **delete protocols bgp neighbor maximum-prefix** command disables the maximum number of prefixes limit.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **ipv4-unicast maximum-prefix** <*max-prefix-number*>

delete protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **ipv4-unicast maximum-prefix** <*max-prefix-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
maximum-prefix <*max-prefix-number*>	Specifies the maximum number of prefixes allowed from the specified neighbor. The value is an integer from 1 to 4294967295. By default, there is no limit for the maximum number of prefixes.

Usage Guidelines

In practice, it is generally preferable to use a prefix-list to limit what prefixes are received from the peer instead of using this knob. Tearing down the BGP session when a limit is exceeded is far more destructive than merely rejecting undesired prefixes. The prefix-list method is also much more granular and offers much smarter matching criterion than number of received prefixes, making it more suited to implementing policy.

Example

• This example sets the prefix limit to 1000 prefixes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast maximum-prefix 1000
admin@XorPlus# commit
```

set protocols bgp neighbor maximum-prefix-out

The **set protocols bgp neighbor maximum-prefix-out** command sets a maximum number of prefixes we can send to a given neighbor. Since sent prefix count is managed by update-groups, this option creates a separate update-group for outgoing updates.
The **delete protocols bgp neighbor maximum-prefix-out** command disables the maximum number of prefixes limit.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **ipv4-unicast maximum-prefix-out** <*max-prefix-number*>

delete protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **ipv4-unicast maximum-prefix-out** <*max-prefix-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
maximum-prefix-out <*max-prefix-number*>	Specifies the maximum number of prefixes we can send to a given neighbor. The value is an integer from 1 to 4294967295. By default, there is no limit for the maximum number of prefixes.

Example
• This example sets the prefix limit we can send to a given neighbor to 1000 prefixes.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 ipv4-unicast maximum-prefix-out 1000
admin@XorPlus# commit
```

set protocols bgp neighbor port

The **set protocols bgp neighbor port** command sets a custom TCP port of the neighbor on which to communicate with the BGP neighbor.
The **delete protocols bgp neighbor port** command allows a random TCP port to be selected for the communication with the BGP neighbor.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **port** <*port-number*>

delete protocols bgp [**vrf** <*vrf-name*>] **neighbor** <*ip*> **port** <*port-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
port <*port-number*>	Specifies a TCP port number. The value is an integer that ranges from 0 to 65535.

Example
• This example sets the TCP port of the neighbor to 1500.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 port 1500
admin@XorPlus# commit
```

set protocols bgp neighbor sender-as-path-loop-detection

The **set protocols bgp neighbor sender-as-path-loop-detection** command enables the detection of sender side AS path loops and filter the bad routes before they are sent. This setting is disabled by default.
The **delete protocols bgp neighbor sender-as-path-loop-detection** command removes the configuration.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} sender-as-path-loop-detection**

delete protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} sender-as-path-loop-detection**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example
• This example enables the detection of sender side AS path loops and filter the bad routes before they are sent.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 sender-as-path-loop-detection
admin@XorPlus# commit
```

set protocols bgp fast-external-failover

The **set protocols bgp fast-external-failover** command can be used to set the switch to reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down.
The **delete protocols bgp fast-external-failover** command turns off this ability.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **fast-external-failover**

delete protocols bgp [***vrf*** <*vrf-name*>] **fast-external-failover**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example
• This example sets the switch to reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down.

```
admin@XorPlus# set protocols bgp fast-external-failover
admin@XorPlus# commit
```

set protocols bgp confederation identifier

The **set protocols bgp confederation identifier** command configures a BGP confederation with the confederation identifier. The group of Autonomous Systems (ASs) will be presented as a single autonomous system with the confederation identifier as the AS number.
The **delete protocols bgp confederation identifier** command deletes the BGP confederation identifier.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **confederation identifier** <*as-number*>

delete protocols bgp [***vrf*** <*vrf-name*>] **confederation identifier** <*as-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
identifier <*as-number*>	Specifies the identifier for the confederation. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example
• This example sets the BGP confederation with the AS number.

```
admin@XorPlus# set protocols bgp confederation identifier 55530
admin@XorPlus# commit
```

set protocols bgp confederation peers

The **set protocols bgp confederation peers** command configures BGP confederation peers with both same and different sub-autonomous system to establish an eBGP membership.
The **delete protocols bgp confederation peers** command disables the peer session and deletes the peer information.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **confederation peers** <*as-number*>

delete protocols bgp [***vrf*** <*vrf-name*>] **confederation peers** <*as-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peers <*as-number*>	Specifies the autonomous system number to establish an eBGP membership. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example
• This example configures peers with ASNs.

```
admin@XorPlus# set protocols bgp confederation peers 62341
admin@XorPlus# commit
```

set protocols bgp dampening

The **set protocols bgp ipv4-unicast dampening** command enables (with optionally specified dampening parameters) or disables route-flap dampening for all routes of a BGP instance.
The **delete protocols bgp ipv4-unicast dampening** command deletes the configuration.

Command Syntax

set protocol bgp ipv4-unicast dampening [half-life-timer <*half-timer*> | **maximum-duration** <*max-duration*> | **start-reusing** <*lower-threshold*> | **start-suppressing** <*high-threshold*>]

delete protocols bgp ipv4-unicast dampening half-life-timer [half-life-timer <*half-timer*> | **maximum-duration** <*max-duration*> | **start-reusing** <*lower-threshold*> | **start-suppressing** <*high-threshold*>]

Parameter

Parameter	Description
half-life-timer <*half-timer*>	Optional. Specifies the half-life time in minutes. When the time expires, the penalty on a route gets reduced exponentially to half its current value. The value is an integer that ranges from 1 to 45. The default value is 15 minutes.
maximum-duration <*max-duration*>	Optional. Specifies the maximum duration to suppress a stable route in minutes. The value is an integer that ranges from 1 to 255. The default value is 60 minutes.
start-reusing <*lower-threshold*>	Optional. Specifies the lower threshold of penalty. On a suppressed route, when the penalty on a route falls below this value, the route is unsuppressed. The value is an integer that ranges from 1 to 20000. The default value is 750.
start-suppressing <*high-threshold*>	Optional. Specifies the upper threshold of penalty. When the penalty on a flapping route exceeds this value, the route is suppressed. The value is an integer that ranges from 1 to 20000. The default value is 2000.

Usage Guidelines

The dampening algorithm assigns a penalty of 1000 to a flapping route every time the route gets withdrawn. The penalty values accumulate on the route every time it flaps. However, the penalty decays and is reduced
to half its value by the half-life time.
NOTE: This feature is not applicable on IBGP routes.

Example
• This example enables dampening with optionally specified parameters.

```
admin@XorPlus# set protocol bgp ipv4-unicast dampening half-life-timer 20
admin@XorPlus# set protocol bgp ipv4-unicast dampening start-reusing 850
admin@XorPlus# set protocol bgp ipv4-unicast dampening start-suppressing 2500
admin@XorPlus# set protocol bgp ipv4-unicast dampening 30
admin@XorPlus# commit
```

set protocols bgp default local-preference

The **set protocols bgp default local-preference** command defaults local preference value for BGP learned routes. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.
The **delete protocols bgp default local-preference** command sets the local preference to the default value of 100.

Command Syntax

set protocol bgp [**vrf** <*vrf-name*>] **default local-preference** <*preference-value*>

delete protocols bgp [***vrf*** <*vrf-name*>] **default local-preference** <*preference-value*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
local-preference <*preference-value*>	Specifies the local preference value. The value is an integer that ranges from 0 to 4294967295. The default value is 100.

Example
• This example defaults local preference value for BGP learned routes to 20.

```
admin@XorPlus# set protocols bgp default local-preference 20
admin@XorPlus# commit
```

set protocols bgp as-notation

The **set protocols bgp as-notation** command configures the display format of the 4-byte Autonomous System (AS) numbers be shown for all show commands.

By default, the BGP 4-byte AS number is displayed in the same format as the AS number configured in the **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*> command.

The **delete protocols bgp as-notation** command deletes the configuration.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **as-notation** <**dot | dot+ | plain**>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
dot	Specifies that Autonomous System (AS) numbers greater than 65535 be shown in dotted integer format for all show commands.
dot+	Specifies to force all Autonomous System (AS) numbers to be shown in dotted integer format for all show commands.
plain	Specifies that Autonomous System (AS) numbers be shown in non-dotted, simple integer.

Usage Guidelines

The **set protocols bgp as-notation** command changes the display format of the 4-byte AS number and AS_PATH that appears in the display information of all show commands.

The conversion relationship between 4-byte AS number in integer format (z) and 4-byte AS number in dotted format (x.y) is: z = x * 65536 + y, for example, a 4-byte AS number 10.2 in dotted format, the corresponding 4-byte AS number in integer format is: 10*65536+2=655362.

NOTE :

The **set protocols bgp as-notation** command and the **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*> command must be in the same commit. If you want to configure **as-notation** when the **local-as** configuration has been successfully committed, then you have to remove all the BGP configuration (all **set protocols bgp** xx commands) and then reconfigure to make sure that the **as-notation** command and the **local-as** command are in the same commit.

Example

- Configure the display format of the 4-byte Autonomous System (AS) numbers be shown in dotted integer format for all show commands.

```
admin@PICOS# set protocols bgp local-as 12
admin@PICOS# set protocols bgp as-notation dot+
admin@PICOS# commit
```

set protocols bgp neighbor local-as

The **set protocols bgp neighbor local-as** command configures an alternate local AS number that can be used to establish a session with a peer, allowing a router to appear to be a member of a second autonomous system (AS), and its real AS.

Local AS allows two autonomous systems to merge without modifying peering arrangements. This command is valid only for eBGP peers.

The **delete protocols bgp neighbor local-as** command restores the default, which is for a peering session to be established using the primary AS (primary AS is the real AS number specified at the time of neighbor creation using the command **set protocols bgp local-as**).

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**|peer-group** <*peer-group*>|**interface** <*interface*>**} local-as** <*AS-NUMBER*> [**no-prepend** [**replace-as**]]

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**|peer-group** <*peer-group*>|**interface** <*interface*>**} local-as**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
local-as <*AS-NUMBER*>	Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.
no-prepend [**replace-as**]	Optional. Specifies that the alternate local AS number is not prepended to the AS_PATH in BGP routes. • If the **no-prepend** attribute is specified, then the supplied local-as is not prepended to the received AS_PATH. • If the **replace-as** attribute is specified, then only the supplied local-as is prepended to the AS_PATH when transmitting local-route updates to this peer. Note that replace-as can only be specified if no-prepend is.

Usage Guidelines

Specify an alternate AS for this BGP process when interacting with a specified peer. With no modifiers (**no-prepend** [**replace-as**]), the specified local-as is prepended to the received AS_PATH when receiving routing updates from the peer, and prepended to the outgoing AS_PATH (after the process local AS) when transmitting local routes to the peer.

NOTEs :

- AS number configured by command **set protocols bgp neighbor local-as** cannot be the same as local AS number (configured by command **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*>) or remote AS number of the specified peer.
- For a switch in a BGP confederation, AS number configured in command **set protocols bgp neighbor local-as** cannot be the same as the AS number (configured by command **set protocols bgp** [**vrf** <*vrf-name*>] **local-as** <*AS-NUMBER*>) of any switch in the BGP confederation.

This command is commonly used in scenarios where carriers modify their network deployments. For example, when carrier A acquires carrier B, the AS of carrier B needs to be merged into the AS of carrier A as they are located in different ASes, that is, the AS number of the carrier B is modified to the AS number of carrier A. However, during the network consolidation process, BGP peers of the original carrier B located in other ASs may not expect or be inconvenient to modify the local BGP configuration immediately, which may result in a loss of connectivity with these peers.

To ensure successful network consolidation progress, you can set the original AS number of carrier B as an alternate local AS number on carrier B by using command **set protocols bgp neighbor local-as**, which allows carrier B to keep connection with other BGP peers using the alternate AS number.

Example

- Configure an alternate local AS number that can be used to establish a session with an eBGP peer.

```
admin@PICOS# set protocols bgp neighbor 100.1.1.134 local-as 200
admin@PICOS# commit
```

OSPFv2 Commands

- run clear ospf interface
- run show ospf border-routers
- run show ospf database
- run show ospf interface
- run show ospf neighbor
- run show ospf route
- run show ospf summary-address
- set protocols ospf aggregation timer
- set protocols ospf area area-type
- set protocols ospf area filter-list prefix
- set protocols ospf area no-summary
- set protocols ospf area range
- set protocols ospf area virtual-link
- set protocols ospf area virtual-link authentication
- set protocols ospf area virtual-link authentication-key
- set protocols ospf area virtual-link dead-interval
- set protocols ospf area virtual-link hello-interval
- set protocols ospf area virtual-link message-digest-key md5
- set protocols ospf area virtual-link retransmit-interval
- set protocols ospf area virtual-link transmit-delay
- set protocols ospf auto-cost reference-bandwidth
- set protocols ospf compatible rfc1583
- set protocols ospf default-information originate
- set protocols ospf default-metric
- set protocols ospf interface area
- set protocols ospf interface authentication-key
- set protocols ospf interface authentication message-digest
- set protocols ospf interface cost
- set protocols ospf interface dead-interval
- set protocols ospf interface hello-interval
- set protocols ospf interface message-digest-key md5
- set protocols ospf interface network
- set protocols ospf interface priority
- set protocols ospf interface retransmit-interval
- set protocols ospf interface transmit-delay
- set protocols ospf log-adjacency-changes
- set protocols ospf max-metric router-lsa administrative
- set protocols ospf max-metric router-lsa on-shutdown
- set protocols ospf max-metric router-lsa on-startup
- set protocols ospf multi-instance disable
- set protocols ospf network area
- set protocols ospf passive-interface
- set protocols ospf redistribute
- set protocols ospf redistribute metric-type
- set protocols ospf redistribute route-map
- set protocols ospf router-id
- set protocols ospf summary-address
- set protocols ospf timers lsa min-arrival
- set protocols ospf timers throttle spf
- set protocols ospf traceoption ism
- set protocols ospf traceoption lsa
- set protocols ospf traceoption nsm
- set protocols ospf traceoption packet
- set protocols ospf traceoption zebra
- set protocols ospf graceful-restart enable
- set protocols ospf capability opaque
- set protocols ospf graceful-restart grace-period
- set protocols ospf graceful-restart helper enable
- set protocols ospf graceful-restart helper planned-only
- set protocols ospf graceful-restart helper strict-lsa-checking
- set protocols ospf graceful-restart helper supported-grace-time

- run graceful-restart prepare ospf
- run show ospf graceful-restart helper

run clear ospf interface

Run the command **clear ospf interface** to clear or reset adjacency with the neighbor session. The specified interface should be a layer 3 interface.

Command Syntax

run clear ospf interface <*l3-interface*>

Parameter

Parameter	Description
interface <*l3-interface*>	Specifies the layer 3 interface. The value is a string.

Example

- Clear OSPF interface *vlan100*.

```
admin@XorPlus# run clear ospf interface vlan100
admin@Xorplus# commit
```

run show ospf border-routers

Run the command **run show ospf border-routers** to display OSPF ABRs and ASBRs.

If OSPF is running in multiple instance then add the instance ID parameter to the command to display ABRs and ASBRs within a particular OSPF instance.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf<***vrf-name***>] border-routers**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the VRF name, the value is a string.

Example

- Display ABRs and ASBRs in OSPF instance ID 1.

```
admin@switch1# run show ospf instance-id 1 border-routers
OSPF Instance: 1
============ OSPF router routing table =============
R    3.3.3.3               [10] area: 1.1.1.1, ASBR
                           via 11.251.201.4, vlan11
```

run show ospf database

To display the OSPF database, run the command **run show ospf database.** To display OSPF database summary, add the argument **summary** to the command.

If OSPF is running in multiple VRFs then add the parameter VRF to display OSPF database for the specified VRF. If multi-instance OSPF is running then add the instance ID to check the OSPF database for that instance.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf**<*vrf-name*>**] database [summary]**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name*>	Optional. Specifies the VRF name, the value is a string.

Example

- Display the OSPF database for vrf1.

```
admin@switch1# run show ospf vrf vrf1 database
VRF Name: vrf1

       OSPF Router with ID (1.1.1.1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          328 0x80000017 0xf095 1
2.2.2.2         2.2.2.2          405 0x80000018 0xadcf 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.251.201.3    2.2.2.2          345 0x80000014 0x89d6

                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
11.251.201.0    1.1.1.1          388 0x80000014 0x80ea 11.251.201.0/24

                ASBR-Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
3.3.3.3         1.1.1.1          908 0x80000010 0xfa38

                Router Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         1058 0x8000001a 0x0779 1
3.3.3.3         3.3.3.3         1087 0x8000001b 0x8be0 1

                Net Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum
11.251.201.4    3.3.3.3         1067 0x80000014 0x86cf

                Summary Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Route
```

```
10.251.201.0    1.1.1.1          378 0x80000014 0x8dde 10.251.201.0/24

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         3.3.3.3         1607 0x80000010 0x7442 E2 0.0.0.0/0 [0x0]
```

To display OSPF database of an OSPF instance, run the command below

```
admin@Xorplus# run show ospf instance-id 1 database
OSPF Instance: 1

       OSPF Router with ID (41.41.41.41)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
41.41.41.41     41.41.41.41      119 0x80000003 0x3454 1

                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.1.0     41.41.41.41      159 0x80000001 0x4004 192.168.1.0/24

                Router Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
41.41.41.41     41.41.41.41      119 0x80000003 0xd9b8 1

                Summary Link States (Area 1.1.1.1)

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.11.0    41.41.41.41      159 0x80000001 0xd168 192.168.11.0/24
```

run show ospf interface

Run the command **run show ospf interface** to display information about layer 3 interfaces participating in OSPF process. The command output displays information such as interface name, IP address, the area this interfaces belongs to, neighbor adjacency count, multicast group memberships and OSPF timers etc.

To display the interface traffic related to OSPF, add the argument **traffic** to the command. This will display information such as OSPF hello messages sent and received on the interface, database description messages sent and received etc. You can also specify a particular interface to show information related to that L3 interface.

If OSPF is running in the default VRF then no need to specify the VRF but if OSPF is running in a user defined VRF then you need to specify the VRF by using the **vrf** parameter.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf<***vrf-name***>] interface** [**traffic | an-interface** <*vlan-interface*>]

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the name of the VRF. The value is a string.
interface<traffic>	Show traffic related to OSPF interfaces.
an-interface <*vlan-interface*>	Specify a L3 interface, the value is a string. It can be the VLAN interface name, the routed interface or the sub-interface name.

Example

- Show OSPF interface related information in OSPF instance ID 1.

```
admin@Xorplus# run show ospf instance-id 1 interface
OSPF Instance: 1

vlan111 is up
  ifindex 257, MTU 1500 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
  Internet Address 192.168.1.11/24, Broadcast 192.168.1.255, Area 1.1.1.1
  MTU mismatch detection: enabled
  Router ID 41.41.41.41, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  No backup designated router on this network
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 8.646s
  Neighbor Count is 1, Adjacent neighbor count is 0
vlan1111 is up
  ifindex 265, MTU 1500 bytes, BW 0 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
  Internet Address 192.168.11.2/24, Broadcast 192.168.11.255, Area 0.0.0.0
  MTU mismatch detection: enabled
  Router ID 41.41.41.41, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  No backup designated router on this network
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
    Hello due in 3.016s
  Neighbor Count is 1, Adjacent neighbor count is 0
```

run show ospf neighbor

Run the command **run show ospf neighbor** to display the OSPF neighbor devices. The command output displays the neighbor router ID, State, Dead Time, Address and Interface etc.

If OSPF is running in the default VRF then no need to specify the VRF but if OSPF is running in a user defined VRF then you need to specify the VRF by using the **vrf** parameter.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

If you require more detail about OSPF neighbors then add the argument **detail** to the command which will display information about the OSPF area the neighbor belongs to and recent state change statistics etc.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] neighbor [detail]**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Specifies the VLAN interface name.

Example

- The command below displays OSPF neighbors (two) for switch1 in vrf1.

```
admin@switch1# run show ospf vrf vrf1 neighbor
VRF Name: vrf1

Neighbor ID     Pri State           Dead Time Address         Interface                        RXmtL RqstL DBsmL
2.2.2.2           1 Full/DR           38.590s 10.251.201.3    vlan10:10.251.201.2                  0     0     0
3.3.3.3           1 Full/DR           30.605s 11.251.201.4    vlan11:11.251.201.2                  0     0     0



admin@switch1# run show ospf vrf vrf1 neighbor detail
VRF Name: vrf1
 Neighbor 2.2.2.2, interface address 10.251.201.3
    In the area 0.0.0.0 via interface vlan10
    Neighbor priority is 1, State is Full, 6 state changes
    Most recent state change statistics:
      Progressive change 57m32s ago
    DR is 10.251.201.3, BDR is 10.251.201.2
    Options 2 *|-|-|-|-|-|E|-
    Dead timer due in 37.160s
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission on
    Thread Link State Update Retransmission on

 Neighbor 3.3.3.3, interface address 11.251.201.4
    In the area 1.1.1.1 via interface vlan11
    Neighbor priority is 1, State is Full, 6 state changes
    Most recent state change statistics:
      Progressive change 57m30s ago
    DR is 11.251.201.4, BDR is 11.251.201.2
    Options 2 *|-|-|-|-|-|E|-
    Dead timer due in 39.177s
    Database Summary List 0
```

```
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission on
    Thread Link State Update Retransmission on

To see the OSPF neighbors in an OSPF instance, run the command below

admin@Xorplus# run show ospf instance-id 1 neighbor
OSPF Instance: 1


Neighbor ID     Pri State           Dead Time Address         Interface                          RXmtL RqstL DBsmL
81.81.81.81       1 Init/DROther      36.580s 192.168.1.12    vlan111:192.168.1.11                   0     0     0
171.171.171.171   1 Init/DROther      35.310s 192.168.11.1    vlan1111:192.168.11.2                  0     0     0
```

run show ospf route

Run the command **run show ospf route** to display OSPF routes in the routing table.

If OSPF is running in the default VRF then no need to specify the VRF but if OSPF is running in a user defined VRF then you need to specify the VRF by using the **vrf** parameter.

Add the optional parameter **instance-id** to show routes of a specific OSPF instance in the default VRF.

Command Syntax

run show ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] route**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
vrf <vrf-name>	Optional. Specifies the VRF name. The value is a string.

Example

- Display OSPF routes of switch1 in vrf1.

```
admin@switch1# run show ospf vrf vrf1 route
VRF Name: vrf1
============ OSPF network routing table ============
N    10.251.201.0/24       [10] area: 0.0.0.0
                           directly attached to vlan10
N    11.251.201.0/24       [10] area: 1.1.1.1
                           directly attached to vlan11

============ OSPF router routing table =============
R    3.3.3.3               [10] area: 1.1.1.1, ASBR
                           via 11.251.201.4, vlan11

============ OSPF external routing table ===========
N E2 0.0.0.0/0             [10/1] tag: 0
                           via 11.251.201.4, vlan11



admin@Xorplus# run show ospf instance-id 1 route
OSPF Instance: 1

============ OSPF network routing table ============
N    192.168.1.0/24        [10] area: 1.1.1.1
                           directly attached to vlan111
N    192.168.11.0/24       [10] area: 0.0.0.0
                           directly attached to vlan1111
```

run show ospf summary-address

The **run show ospf summary-address** command shows the configuration for display all configured summary routes with matching external LSA information.

Command Syntax

run show ospf summary-address [detail]

Parameters

Parameter	Description
detail	Optional. Shows a detailed view of all configured summary routes with matching external LSA information.

Example

- The following commands shows the configuration for display all configured summary routes with matching external LSA information.

```
admin@Xorplus# run show ospf summary-address
Summary-address     Metric-type     Metric     Tag         External_Rt_count
aggregation delay interval :100(in seconds)
10.10.0.0/16          E2            20         1234        0
```

set protocols ospf aggregation timer

The **set protocols ospf aggregation timer** command configures ASBR route summarization delay timer interval. Summarization starts only after this delay timer expiry.

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] aggregation timer** <*aggregation-timer*>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
Aggregation timer <*aggregation-timer*>	Specifies delay timer for starting ASBR route summarization. The value is an integer that ranges from 5 to 1800, in seconds. The default value is 5 seconds.

Example

- The following commands changes the ASBR route summarization delay timer to 100 seconds.

```
admin@Xorplus# set protocols ospf aggregation timer 100
admin@Xorplus# commit
```

set protocols ospf area area-type

Run the command **set protocols ospf area area-type** to define an OSPF area type. Two types of areas can be specified here. To create a stub area, choose the key word **stub**, or choose **nssa**, to create OSPF *not-so-stubby-area.* Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf area stub** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf**<*vrf-name*>**] area {**<*ipv4*>**|**<*area-id*>**} area-type <stub|nssa>**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>**|**<*area-id*>**} area-type <stub|nssa>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specify OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
stub	Keyword to specify a stub area.
nssa	Keyword to specify a not-so-stubby-area.

Example

- Configure area 1.1.1.1 in the default VRF as a stub area.

```
admin@XorPlus# set protocols ospf instance-id 1 area 1.1.1.1 area-type stub
admin@Xorplus# commit
```

set protocols ospf area filter-list prefix

Run the command **set protocols ospf area filter-list prefix** to create a filter list which acts as an access list for route advertisement in OSPF. This command filters Type-3 summary-LSAs to or from area using prefix lists. Keywords **in** or **out** is used to specify the inbound or outbound direction for the filter list. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf area filter-list prefix** to delete this configuration.

Command Syntax.

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} {in|out} filter-list prefix** <*prefix-list-v4*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} {in|out} filter-list prefix** <*prefix-list-v4*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
prefix <*prefix-list*>	Specifies the filter list name.
in	Specifies the inbound direction.
out	Specifies the outbound direction.

Example

- Configure prefix list1 for VRF BLUE, area 1.1.1.1 in the outbound direction.

```
admin@XorPlus# set protocols ospf vrf BLUE area 1.1.1.1 out prefix-list prefix list1
admin@Xorplus# commit
```

set protocols ospf area no-summary

Run the command **set protocols ospf area** to define an OSPF area and disallow injecting inter-area routes. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. The keyword **no-summary** is used to disable injecting inter-area summaries into the specified stub area. The **no-summary** option makes the area totally stubby.

> Multi-Instance OSPF is only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf area** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] area {**<*ipv4*>**|**<*area-id*>**} no-summary**

delete protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] area {**<*ipv4*>**|**<*area-id*>**} no-summary**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
no-summary	Keyword to disable injecting inter-area summaries into the specified stub area.

Example

- Configure area 1.1.1.1 in for instance ID 1 in the default VRF and disable injecting inter-area summaries into this area.

```
admin@XorPlus# set protocols ospf instance-id 1 area 1.1.1.1 no-summary
admin@Xorplus# commit
```

set protocols ospf area range

The **set protocols ospf area range** command summarizes intra area paths from specified area into a single Type-3 summary-LSA announced to other areas. This command can be used only on ABR and ONLY router-LSAs (Type-1) and network-LSAs (Type-2, i.e. LSAs with scope area) can be summarized.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] area {**<*ipv4*>|<*area-id*>**} range** <*prefix/mask*> [**advertise** <**true | false**> **| cost** <*cost*> **| substitute** <*prefix/mask*>]

Parameters

Parameter	Description
instance-id <*instance-id*>	Optional. Specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be in IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
range <*prefix/mask*>	Specifies summarizing routes matching the area range *prefix/mask*.
advertise <true | false>	Optional. Determines whether to advertise the summarized route or not. The value could be **true** or **false**. • **true**: Advertise the summarized route. • **false**: Do not advertise the summarized route. By default, the summarized route is advertised.
cost <*cost*>	Optional. Specifies the cost of the summarized route. The value is an integer that ranges from 0 to 16777215.
substitute <*prefix/mask* >	Optional. Specifies another prefix to substitute the already configured one to announce to other areas.

Example

- The following commands configure route summarization in OSPF area 1.

```
admin@Xorplus# set protocols ospf area 1 range 10.42.0.0/16
admin@Xorplus# commit
```

set protocols ospf area virtual-link

The **set protocols ospf area virtual-link** command creates an OSPF virtual link with a remote ABR and enters the vlink context.

The **delete protocols ospf area virtual-link** command deletes an OSPF virtual link with the specified router ID of the remote ABR. If no *<ROUTER-ID>* is specified, the command sets the virtual link to the default settings.

Command Syntax

set protocols ospf [**vrf** *<vrf-name>*] **area {***<ipv4>*|*<area-id>***} virtual-link** *<ROUTER-ID>*

Parameters

Parameter	Description
vrf *<vrf-name>*	Optional. Specifies the name of the VRF for the OSPF instance.
area {*<ipv4>*|*<area-id>*}	Specifies the OSPF area ID. The value could be in IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link *<ROUTER-ID>*	Configures a virtual link with the specified router ID of the remote ABR.

Example

- Configuring OSPF virtual links:

```
admin@Xorplus# set protocols ospf area 1 virtual-link 100.0.1.1
admin@Xorplus# commit
```

set protocols ospf area virtual-link authentication

Run the command **set protocols ospf area virtual-link authentication** to set the OSPF virtual-link authentication type that will be used for authentication with the remote ABR.

The command **delete protocols ospf area virtual-link authentication** unconfigures the virtual-link authentication type used and sets it to Null authentication, means no authentication.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication** [<**message-digest | null**>]

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication** [<**message-digest | null**>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
authentication [<**message-digest | null**>]	Choose one of the authentication types from the following parameters. • **message-digest:** Optional. Sets the authentication type to message-digest. • **null**: Optional. Sets the authentication type to null, means no authentication. If no authentication types is specified, the simple-text authentication type will be used.

Usage Guidelines

The authentication modes and passwords of all the devices must be the same in any given area, but can differ between several areas.

When authentication type **message-digest** is configured, command set protocols ospf area virtual-link message-digest-key md5 can be used to set the md5 password.

When using **simple-text** authentication type, command set protocols ospf area virtual-link authentication-key can be used to set the password.

Example

- Configure OSPF virtual links authentication type:

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 authentication message-digest
admin@Xorplus# commit
```

set protocols ospf area virtual-link authentication-key

Run the command **set protocols ospf area virtual-link authentication-key** to set the OSPF virtual-link authentication password that is used for simple-text authentication.

The command **delete protocols ospf area virtual-link authentication-key** deletes the virtual-link authentication password that is used for simple-text authentication.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication-key** <*PASSWORD*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **authentication-key**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
authentication-key <*PASSWORD*>	Specifies the password for simple-text authentication. The value is a string of 6 to 8 characters.

Example

- Configure OSPF virtual links authentication password:

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 authentication-key afsjlfk
admin@Xorplus# commit
```

set protocols ospf area virtual-link dead-interval

Run the command **set protocols ospf area virtual-link dead-interval** to configure the OSPF neighbor router of a virtual link dead interval in seconds. This value must be the same on all routers in the OSPF domain.

Run the command **delete protocols ospf area virtual-link dead-interval** to remove this configuration and revert to the default value which is 40 seconds.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **dead-interval** <*seconds*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **dead-interval**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
dead-interval <*seconds*>	Specifies the OSPF neighbor dead interval in seconds. The value ranges from 1 to 65535. The default interval is 40 seconds.

Example

- Configure the OSPF neighbor dead interval to 60 seconds.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 dead-interval 60
admin@Xorplus# commit
```

set protocols ospf area virtual-link hello-interval

Run the command **set protocols ospf area virtual-link hello-interval** to set the OSPF hello interval on the virtual link. Hello packets will be sent every **hello-interval** of time. The default value is 10 seconds.

Run the command **delete protocols ospf area virtual-link hello-interval** to remove this configuration and revert back to the default 10 seconds.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **hello-interval** <*seconds*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **hello-interval** <*seconds*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
hello-interval <*seconds*>	Specifies the hello interval in seconds. The value ranges from 1 to 65535. The default value is 10 seconds.

Example

- Configure the hello interval to 60 seconds on the virtual link.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 hello-interval 60
admin@Xorplus# commit
```

set protocols ospf area virtual-link message-digest-key md5

Run the command **set protocols ospf area virtual-link message-digest-key md5** to set OSPF authentication key to a cryptographic password. The cryptographic algorithm is MD5. The key number can be any digit between 1 and 255.

Note: Its important to configure the same key number and password on both ends for the OSPF authentication to be successful.

To delete the configuration, run the command **delete protocols ospf area virtual-link message-digest-key md5**.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **message-digest-key** <*1-255*> **md5** <*password*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **message-digest-key** <*1-255*> **md5** <*password*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
message-digest-key <*1-255*>	Specifies the MD5 key ID. The value is an integer in the range of 1 to 255.
md5 <*password*>	Specifies the MD5 authentication password that is used for message-digest authentication. The value is a string of 6 to 16 characters.

Usage Guidelines

The authentication modes and passwords of all the devices must be the same in any given area, but can differ between several areas.

PicOS recommends you configure only one set of **message-digest-key** and **md5** password.

Example

- Configure MD5 key ID as 1.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 message-digest-key 1 md5 wrwgdygd
admin@Xorplus# commit
```

set protocols ospf area virtual-link retransmit-interval

Run the command **set protocols ospf area virtual-link retransmit-interval** to set the time between retransmitting lost link state advertisements for the OSPF virtual link.
The command **delete protocols ospf area virtual-link retransmit-interval** sets the time between retransmitting lost link state advertisements to the default of 5 seconds for the OSPF virtual link.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **retransmit-interval** <*INTERVAL*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **retransmit-interval**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
retransmit-interval <*INTERVAL*>	Specifies the retransmit interval, in seconds. Range: 1 to 65535. Default: 5.

Example

- Configure the OSPF retransmit interval for the OSPF virtual link.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 retransmit-interval 30
admin@Xorplus# commit
```

set protocols ospf area virtual-link transmit-delay

Run the command **set protocols ospf area virtual-link transmit-delay** to set the time delay in link state transmission for the OSPF virtual link.
The command **delete protocols ospf area virtual-link transmit-delay** sets the delay in link state transmission to the default of 1 second for the OSPF virtual link.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **transmit-delay** <*DELAY*>

delete protocols ospf [**vrf** <*vrf-name*>] **area {**<*ipv4*>**|**<*area-id*>**} virtual-link** <*ROUTER-ID*> **transmit-delay**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
area {<*ipv4*>|<*area-id*>}	Specifies the OSPF area ID. The value could be IPv4 dotted decimal format or an integer that ranges from 0 to 4294967295.
virtual-link <*ROUTER-ID*>	Configures a virtual link with the specified router ID of the remote ABR.
transmit-delay <*DELAY*>	Specifies the transit delay in seconds. Range: 1 to 65535. Default: 1.

Example

- Configure the OSPF transmit delay on the virtual link.

```
admin@XorPlus# set protocols ospf area 1.1.1.1 virtual-link 100.0.1.1 transmit-delay 30
admin@Xorplus# commit
```

set protocols ospf auto-cost reference-bandwidth

Run the command **set protocols ospf auto-cost reference-bandwidth** to set the reference bandwidth for automatic route cost calculation. The reference bandwidth specified here is considered equivalent to OSPF cost of 1. The default bandwidth is 100Mbits/s, that is, a link with bandwidth of 100Mbits/s or higher is considered to have a cost of 1. Cost of links with lower bandwidth will be calculated with reference to this bandwidth value. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional parameter **vrf** can be used to specify the name of the VRF for the OSPF instance.

Note that this configuration must be consistent within the OSPF domain.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf auto-cost reference-bandwidth** to delete this configuration

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] auto-cost reference-bandwidth** <*ref-bandwidth*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>***] auto-cost reference-bandwidth** <*ref-bandwidth*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
reference-bandwidth <*ref-bandwidth*>	Specifies the reference bandwidth. The value is an integer that ranges from 1 to 4294967.

Example

- Configure the OSPF reference bandwidth to 500000 for the default VRF OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 auto-cost reference-bandwidth 500000
admin@Xorplus# commit
```

set protocols ospf compatible rfc1583

Run the command **set protocols ospf compatible rfc1583** to enable OSPF compatibility with RFC1583 (backward compatibility). If RFC1583 compatibility is enabled, then the route cost calculation follows a different method.

Run the command **delete protocols ospf compatible** to delete this configuration.

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] compatible rfc1583**

delete protocols ospf [vrf <*vrf-name*>**] compatible**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Example

- Enable OSPF RFC1583 compatibility:

```
admin@XorPlus# set protocols ospf vrf BLUE compatible rfc1583
admin@Xorplus# commit
```

set protocols ospf default-information originate

Run the command **set protocol ospf default-information originate** to originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional keyword **vrf** specifies the name of the VRF for the OSPF instance. If the optional keyword **always** is given then the default route is always advertised, even when there is no default route present in the routing table.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocol ospf default-information originate** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] default-information originate [always]**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] default-information originate [always]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
always	Optional keyword that specifies that the default route is always advertised regardless if its present in the routing table.

Example

- Configure the device to always originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas.

```
admin@XorPlus# set protocols ospf instance-id 1 default-information originate always
admin@Xorplus# commit
```

set protocols ospf default-metric

Run the command **set protocols ospf default-metric** to set the default metric for redistributed routes in the OSPF.
The command **delete protocols ospf default-metric** sets the default metric to be used for redistributed routes into OSPF to the default of 20.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **default-metric** <*METRIC-VALUE*>

delete protocols ospf [**vrf** <*vrf-name*>] **default-metric**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
default-metric <*METRIC-VALUE*>	Specifies the default metric value to use for redistributed routes. The value could be an integer that ranges from 0 to 1677214. The default value is 20.

Example

- Configure default metric for redistributed routes:

```
admin@XorPlus# set protocols ospf default-metric 37
admin@Xorplus# commit
```

set protocols ospf interface area

To enable OSPF on an interface and assign the interface to an area, use the **set protocols ospf interface area** command in L2/L3 configuration mode. The interface will send and accept OSPF LSAs (link-state advertisements). Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

Run the command **delete protocols ospf interface area** to remove this configuration from the system.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] interface** <*interface-name*> **area {**<*ipv4*>|<*area-id*>**}**

delete protocols ospf [instance-id <*instance-id***>] interface** <*interface-name*> **area {**<*ipv4*>|<*area-id*>**}**

Parameters

Parameter	Description
instance-id <*instance-id***>**	Optional. Specifies the OSPF instance ID in the default VRF. The value is an integer that ranges from 1 to 8.
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
area {<*ipv4*>|<*area-id*>**}**	Specifies the OSPF area in IPv4 format or an integer in the range of 0 to 4294967295.

Usage Guidelines

The OSPF commands **set protocols ospf interface area** and **set protocols ospf network area** cannot be configured simultaneously. The user can enable OSPF for either an interface or netowrk, but not both. If one of the two commands has been configured on the device and the user tries to commit the different method of enabling OSPF will result in commit failed error message.

The user must delete the configuration method previously committed before trying to commit the different method and keep the following points in mind:

- If **set protocols ospf network area** has been configured on the device first, you have to delete it before configuring command **set protocols ospf interface area**.
- If **set protocols ospf interface area** has been configured on the device first, and if the configuration is in a specified VRF, you have to delete all OSPF configurations under the specified VRF before configuring the command **set protocols ospf vrf network area**. Or if these configurations are in the default VRF, you have to delete all OSPF configurations of ***all*** VRFs on the device by using command **delete protocols ospf** before configuring **set protocols ospf network area**.

Example

- Enable OSPF on interface vlan200 and assign it to area 1.1.1.1 for instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 interface vlan200 area 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf interface authentication-key

Run the command **set protocols ospf interface authentication-key** to set the authentication password that is used for simple-text authentication on the OSPF interface.
The command **delete protocols ospf interface authentication-key** deletes the OSPF interface authentication password that is used for simple-text authentication.

Command Syntax

set protocols ospf interface <*interface-name*> **address** <*ipv4*> **authentication-key** <*PASSWORD*>

delete protocols ospf interface <*interface-name*> **address** <*ipv4*> **authentication-key**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Specifies an IPv4 address.
authentication-key <*PASSWORD*>	Specifies the password for simple-text authentication. The value is a string of 6 to 8 characters.

Example

- Configure OSPF authentication password on the interface address.

```
admin@XorPlus# set protocols ospf interface vlan200 address 10.10.114.1 authentication-key asjlfk
admin@Xorplus# commit
```

set protocols ospf interface authentication message-digest

Run the command **set protocols ospf interface authentication message-digest** to specify that OSPF packets must be authenticated with MD5 HMACs on the given interface.

Note that you must first create MD5 key using the command **set protocols ospf interface message-digest-key** <1-255> **md5** <key-string> before you can enable MD5 authentication on the interface.

Command Syntax

set protocols ospf interface <*interface-name*> **authentication message-digest**

delete protocols ospf interface <*interface-name*> **authentication message-digest**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Example

- Enable MD5 authentication on interface vlan200.

```
admin@XorPlus# set protocols ospf interface vlan200 authentication message-digest
admin@Xorplus# commit
```

set protocols ospf interface cost

Run the command **set protocols ospf interface cost** to set the OSPF link cost for the specified interface. The cost value is set to router-LSA's metric field and used for SPF calculation. Changing the interface cost causes the OSPF to run the SPF and reissue LSAs.

Run the command **delete protocols ospf interface cost** to remove this configuration.

Command Syntax

set protocols ospf interface <*interface-name*> **cost** <*1-65535*>

delete protocols ospf interface <*interface-name*> **cost**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
cost <*1-65535*>	Specifies the link cost, the value is an integer in the range of 1 to 65535.

Example

- Configure the OSPF interface vlan200 cost to 5.

```
admin@XorPlus# set protocols ospf interface vlan200 cost 5
admin@Xorplus# commit
```

set protocols ospf interface dead-interval

Run the command **set protocols ospf interface dead-interval** to configure the OSPF neighbor router dead interval in seconds. This value must be the same on all routers in the OSPF domain.

Run the command **delete protocols ospf interface dead-interval** to remove this configuration and revert to the default value which is 40 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **dead-interval** <*seconds*>

delete protocols ospf interface <*interface-name*> **dead-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
dead-interval <*seconds*>	Specifies the OSPF neighbor dead interval in seconds. The value ranges from 1 to 65535. The default interval is 40 seconds.

Example

- Configure the OSPF neighbor dead interval to 60 seconds.

```
admin@XorPlus# set protocols ospf interface vlan200 dead-interval 60
admin@Xorplus# commit
```

set protocols ospf interface hello-interval

Run the command **set protocols ospf interface hello-interval** to set the OSPF hello interval on the specified interface. Hello packets will be sent every **hello-interval** of time. The default value is 10 seconds.

Run the command **delete protocols ospf interface hello-interval** to remove this configuration and revert back to the default 10 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **hello-interval** <*seconds*>

delete protocols ospf interface <*interface-name*> **hello-interval** <*seconds*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
hello-interval <*seconds*>	Specifies the hello interval in seconds. The value ranges from 1 to 65535. The default value is 10 seconds.

Example

- Configure the hello interval to 60 seconds on interface vlan200.

```
admin@XorPlus# set protocols ospf interface vlan200 hello-interval 60
admin@Xorplus# commit
```

set protocols ospf interface message-digest-key md5

Run the command **set protocols ospf interface message-digest-key md5** to specify the MD5 key number and password for MD5 authentication for a given interface. The key number can be any digit between 1 and 255. The password string can be any string without spaces, the maximum length of the string should be 16 characters.

Note: Its important to configure the same key number and password on both ends for the OSPF authentication to be successful.

To delete the configuration, run the command **delete protocols ospf interface message-digest-key.**

Command Syntax

set protocols ospf interface <*interface-name*> **message-digest-key** <*1-255*> **md5** <*password*>

delete protocols ospf interface <*interface-name*> **message-digest-key** <*1-255*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
message-digest-key <*1-255*>	Specifies the MD5 key ID. The value is an integer in the range of 1 to 255
md5 <*text*>	Specifies the MD5 key string, the maximum length should not exceed 16 characters and should not have spaces.

Example

- Configure MD5 key ID as 1 and password string as testkey.

```
admin@XorPlus# set protocols ospf interface vlan200 message-digest-key 1 md5 testkey
admin@Xorplus# commit
```

set protocols ospf interface network

Run the command **set protocols ospf interface network** to enable OSPF on an interface and specify a network type. Enabling OSPF on an interface allows the interface to send and receive LSAs. Four different network types can be specified here namely, **broadcast, non-broadcast, point-to-multipoint** and **point-to-point**.

To delete this configuration, run the command **delete protocols ospf interface network**

Command Syntax

set protocols ospf interface <*interface-name*> **network <broadcast|non-broadcast|point-to-multipoint|point-to-point>**

delete protocols ospf interface <*interface-name*> **network <broadcast|non-broadcast|point-to-multipoint|point-to-point>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
broadcast	Specifies the OSPF broadcast multi-access network.
non-broadcast	Specifies the OSPF NBMA network.
point-to-multipoint	Specifies the OSPF point-to-multipoint network.
point-to-point	Specifies the OSPF point-to-point network.

Example

- Enable OSPF on interface vlan200 and specify network type as point-to-point.

```
admin@XorPlus# set protocols ospf interface vlan200 network point-to-point
admin@Xorplus# commit
```

set protocols ospf interface priority

Run the command **set protocols ospf interface priority** to set the OSPF priority for the interface. The larger the numeric value of the priority, the higher the chances for it to become the designated router. Setting a priority of zero makes the router ineligible to become a designated router or back up designated router. The command **delete protocols ospf interface priority** sets the OSPF priority for the interface to the default of 1.

Command Syntax

set protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **priority** <*PRIORITY-VALUE*>

delete protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **priority**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Optional. Specifies an IPv4 address.
priority <*PRIORITY-VALUE*>	Specifies the OSPF priority value. Range: 0 to 255. Default: 1.

Usage Guidelines

L3 interface can be configured with multiple IP addresses. If you specify an interface and also specify an interface address in this command, the parameters are configured only for the specified IP of that interface. If only the interface is specified but no IP address is specified, the parameters are set for all IPs of the interface.

Example

- Configure the OSPF vlan200 priority to 5.

```
admin@XorPlus# set protocols ospf interface vlan200 priority 5
admin@Xorplus# commit
```

set protocols ospf interface retransmit-interval

Run the command **set protocols ospf interface retransmit-interval** to set the time between retransmitting lost link state advertisements for the OSPF interface. The command **delete protocols ospf interface retransmit-interval** sets the time between retransmitting lost link state advertisements to the default of 5 seconds for the OSPF interface.

Command Syntax

set protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **retransmit-interval** <*INTERVAL*>

delete protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **retransmit-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Optional. Specifies an IPv4 address.
retransmit-interval <*INTERVAL*>	Specifies the retransmit interval, in seconds. Range: 1 to 65535. Default: 5.

Usage Guidelines

L3 interface can be configured with multiple IP addresses. If you specify an interface and also specify an interface address in this command, the parameters are configured only for the specified IP of that interface. If only the interface is specified but no IP address is specified, the parameters are set for all IPs of the interface.

Example

- Configure the OSPF retransmit interval on the interface.

```
admin@XorPlus# set protocols ospf interface vlan200 retransmit-interval 30
admin@Xorplus# commit
```

set protocols ospf interface transmit-delay

Run the command **set protocols ospf interface transmit-delay** to set the time delay in link state transmission for the OSPF interface.
The command **delete protocols ospf interface transmit-delay** sets the delay in link state transmission to the default of 1 second for the OSPF interface.

Command Syntax

set protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **transmit-delay** <*DELAY*>

delete protocols ospf interface <*interface-name*> [**address** <*ipv4*>] **transmit-delay**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4*>	Optional. Specifies an IPv4 address.
transmit-delay <*DELAY*>	Specifies the transit delay in seconds. Range: 1 to 65535. Default: 1.

Usage Guidelines

L3 interface can be configured with multiple IP addresses. If you specify an interface and also specify an interface address in this command, the parameters are configured only for the specified IP of that interface. If only the interface is specified but no IP address is specified, the parameters are set for all IPs of the interface.

Example

- Configure the OSPF transmit delay on the interface.

```
admin@XorPlus# set protocols ospf interface vlan200 transmit-delay 30
admin@Xorplus# commit
```

set protocols ospf log-adjacency-changes

Run the command **set protocols ospf log-adjacency-changes** to log changes in OSPF adjacency state. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. Add the optional **detail** argument to log all changes in adjacency state. Without the **detail** keyword, only changes to full or regressions are logged. You can optionally specify the VRF for the single instance OSPF in the non-default VRF for this command to take effect.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf log-adjacency-changes** to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] log-adjacency-changes [detail]**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] log-adjacency-changes [detail]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
detail	Optional. Specifies to log all changes in adjacency state.

Example

- Configure OSPF to log all adjacency changes for VRF BLUE.

```
admin@XorPlus# set protocols ospf vrf BLUE log-adjacency-changes detail
admin@Xorplus# commit
```

set protocols ospf max-metric router-lsa administrative

The **set protocols ospf max-metric router-lsa administrative** command configures the protocol to advertise a maximum metric (65535) so that other routers do not prefer this router as an intermediate hop in their shortest path first (SPF) calculations.

Enabling this feature administratively allows for administrative intervention for whatever reason, for an indefinite period of time. The command will then take effect until manually deleted.

The **delete protocols ospf max-metric router-lsa administrative** command deletes the configuration.

> **NOTE:**
> **max-metric router-lsa** feature has three configuration methods, the commands are shown as below.
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**
>
> They can be configured separately or simultaneously. When **administrative** is configured with other methods, the configuration of "**administrative**" takes effect.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**

delete protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

The highlighted lines in the following example shows that **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa administrative** is configured for advertising the maximum metric.

```
admin@Xorplus# run show ospf vrf x
VRF Name: x
OSPF Routing Process, Router ID: 10.1.240.0
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 0.539s ago
Last SPF duration 173 usecs
SPF timer is inactive
LSA minimum interval 5000 msecs
LSA minimum arrival 1000 msecs
Write Multiplier set to 20
 Refresh timer 10 secs
Maximum multiple paths(ECMP) supported  256
This router is an ASBR (injecting external routing information)
Number of external LSA 5. Checksum Sum 0x000211ba
Number of opaque AS LSA 0. Checksum Sum 0x00000000
```

```
Number of areas attached to this router: 1
Area ID: 0.0.0.0 (Backbone)
  Number of interfaces in this area: Total: 11, Active: 10
  Originating stub / maximum-distance Router-LSA
    Administratively activated (indefinitely)
  Number of fully adjacent neighbors in this area: 1
  Area has no authentication
  SPF algorithm executed 40 times
  Number of LSA 4
  Number of router LSA 3. Checksum Sum 0x0001a0d5
  Number of network LSA 1. Checksum Sum 0x000068d5
  Number of summary LSA 0. Checksum Sum 0x00000000
  Number of ASBR summary LSA 0. Checksum Sum 0x00000000
  Number of NSSA LSA 0. Checksum Sum 0x00000000
  Number of opaque link LSA 0. Checksum Sum 0x00000000
  Number of opaque area LSA 0. Checksum Sum 0x00000000
```

Example

- Setting to maximize the cost metrics for Router LSA to administrative:

```
admin@Xorplus# set protocols ospf max-metric router-lsa administrative
admin@Xorplus# commit
```

set protocols ospf max-metric router-lsa on-shutdown

The **set protocols ospf max-metric router-lsa on-shutdown** command configures the protocol to advertise a maximum metric (65535) so that other routers do not prefer this router as an intermediate hop in their shortest path first (SPF) calculations. **on-shutdown** <*advert-time*> indicates to advertise a maximum metric in advance of shutdown for the *advert-time* configured in seconds to gracefully excuse itself from the OSPF domain.

The **delete protocols ospf max-metric router-lsa on-shutdown** command advertises the normal cost metrics instead of advertising the maximized cost metric.

> **NOTE:**
> **max-metric router-lsa** feature has three configuration methods, the commands are shown as below.
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**
>
> They can be configured separately or simultaneously. When **administrative** is configured with other methods, the configuration of "**administrative**" takes effect.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown** <*advert-time*>

delete protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
on-shutdown <*advert-time*>	Specifies the time interval to advertise a maximum metric in advance of shutdown. The value is an integer, in seconds, that ranges from 5 to 100.

Usage Guidelines

The highlighted lines in the following example shows that **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown** <*advert-time*> is configured with 100 seconds, and 1 minutes 31 seconds remaining is left for advertising the maximum metric and shutting down the router.

```
admin@Xorplus# run show ospf vrf x
VRF Name: x
OSPF Routing Process, Router ID: 10.1.240.0
Deferred shutdown in progress, 1m31s remaining
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Stub router advertisement is configured
  Enabled for 100s prior to full shutdown
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 8.551s ago
Last SPF duration 201 usecs
SPF timer is inactive
LSA minimum interval 5000 msecs
LSA minimum arrival 1000 msecs
Write Multiplier set to 20
```

Refresh timer 10 secs
Maximum multiple paths(ECMP) supported 256
This router is an ASBR (injecting external routing information)
Number of external LSA 2. Checksum Sum 0x0000d86e
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 0.0.0.0 (Backbone)
Number of interfaces in this area: Total: 11, Active: 10
Originating stub / maximum-distance Router-LSA
Administratively activated (indefinitely)
Number of fully adjacent neighbors in this area: 2
Area has no authentication
SPF algorithm executed 8 times
Number of LSA 6
Number of router LSA 3. Checksum Sum 0x00013603
Number of network LSA 3. Checksum Sum 0x0001509c
Number of summary LSA 0. Checksum Sum 0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
Number of opaque link LSA 0. Checksum Sum 0x00000000
Number of opaque area LSA 0. Checksum Sum 0x00000000

Example

- Setting to maximize the cost metrics for Router LSA on shutdown:

```
admin@Xorplus# set protocols ospf max-metric router-lsa on-shutdown 120
admin@Xorplus# commit
```

set protocols ospf max-metric router-lsa on-startup

The **set protocols ospf max-metric router-lsa on-startup** command configures the OSPF protocol to advertise a maximum metric (65535) so that other routers do not prefer this router as an intermediate hop in their shortest path first (SPF) calculations. The parameter **on-startup** <*advert-time*> indicates to advertise a maximum metric from the time the OSPF neighbor is established for the *advert-time* configured in seconds.

The **delete protocols ospf max-metric router-lsa on-startup** command advertises the normal cost metrics instead of advertising the maximized cost metric. This setting causes the router to be considered in traffic forwarding.

> **NOTE:**
> **max-metric router-lsa** feature has three configuration methods, the commands are shown as below.
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-shutdown** <*advert-time*>
>
> **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa administrative**
>
> They can be configured separately or simultaneously. When **administrative** is configured with other methods, the configuration of "**administrative**" takes effect.

Command Syntax

set protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*>

delete protocols ospf [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
on-startup <*advert-time*>	Specifies the time interval to advertise a maximum metric from the time the OSPF neighbor is established. The value is an integer, in seconds, that ranges from 5 to 86400.

Usage Guidelines

This command is mainly used in the following scenarios:

1. When a new router is added to the OSPF network, but don't want to participate in data forwarding immediately. Then, **max-metric router-lsa on-startup** can be configured to establish the adjacency relationship and converge the network normally, while won't become an alternative path for other existing OSPF paths.
2. When a router is about to be disconnected from the network, to avoid neighbors from failing to detect it and causing a routing black hole, the **max-metric router-lsa on-shutdown** can be configured to enable the neighbors to recalculate the path before shutting down the router, and the data will no longer be forwarded through the router.

After the configuration **on-startup** <*advert-time*> is set, OSPF uses the maximum metric (65535) in the advertising LSA (Link State Advertisement) for the configured <*advert-time*> time when OSPF neighbor is established.

The highlighted lines in the following example shows that **set protocols ospf** [**vrf** <*vrf-name*>] **max-metric router-lsa on-startup** <*advert-time*> is configured with 300 seconds, and 3 minutes 39 seconds remaining is left for advertising the maximum metric.

```
admin@Xorplus# set protocols ospf vrf x max-metric router-lsa on-startup 300
admin@Xorplus# commit


admin@Xorplus# run show ospf vrf x
VRF Name: x
OSPF Routing Process, Router ID: 10.1.240.0
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Stub router advertisement is configured
  Enabled for 300s after start-up
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
```

Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 2
SPF algorithm last executed 1m06s ago
Last SPF duration 95 usecs
SPF timer is inactive
LSA minimum interval 5000 msecs
LSA minimum arrival 1000 msecs
Write Multiplier set to 20
Refresh timer 10 secs
Maximum multiple paths(ECMP) supported 256
This router is an ASBR (injecting external routing information)
Number of external LSA 2. Checksum Sum 0x0000fc5c
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 0.0.0.0 (Backbone)
Number of interfaces in this area: Total: 11, Active: 10
Originating stub / maximum-distance Router-LSA
Active from startup, 3m39s remaining
Number of fully adjacent neighbors in this area: 1
Area has no authentication
SPF algorithm executed 6 times
Number of LSA 5
Number of router LSA 3. Checksum Sum 0x00013649
Number of network LSA 2. Checksum Sum 0x0000f3a3
Number of summary LSA 0. Checksum Sum 0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
Number of opaque link LSA 0. Checksum Sum 0x00000000
Number of opaque area LSA 0. Checksum Sum 0x00000000

Example

- Setting to maximize the cost metrics for Router LSA on startup:

```
admin@Xorplus# set protocols ospf max-metric router-lsa on-startup 300
admin@Xorplus# commit
```

set protocols ospf multi-instance disable

Run the command **set protocols ospf multi-instance disable** to enable or disable OSPF multi-instance mode.

Command Syntax

set protocols ospf multi-instance disable <true | false>

Example

- This example enables OSPF multi-instance on the device.

```
admin@XorPlus# set protocols ospf multi-instance disable false
admin@XorPlus# commit
```

set protocols ospf network area

Run the command **set protocols ospf network area** to configure OSPF instance for the IP subnet prefix with an area address per network. The optional parameter **vrf** can be used to specify OSFP instance for a particular VRF. If VRF is not defined then OSPF instance takes effect for the default VRF.

Run the command **delete protocols ospf network area** to delete this configuration.

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] network** <*ipv4/prefixlen*> **area {**<*ipv4*|<*area-id*>**}**

delete protocols ospf [vrf <*vrf-name*>**] network** <*ipv4/prefixlen*> **area {**<*ipv4*>|<*area-id*>**}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
network <*ipv4/prefixlen*>	Specifies the network prefix and prefix length in IPv4 format.
area {<*ipv4*>|<*area-id*>**}**	Specify OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Usage Guidelines

The OSPF commands **set protocols ospf interface area** and **set protocols ospf network area** cannot be configured simultaneously. The user can enable OSPF for either an interface or netowrk, but not both. If one of the two commands has been configured on the device and the user tries to commit the different method of enabling OSPF will result in commit failed error message.

The user must delete the configuration method previously committed before trying to commit the different method and keep the following points in mind:

- If **set protocols ospf network area** has been configured on the device first, you have to delete it before configuring command **set protocols ospf interface area**.
- If **set protocols ospf interface area** has been configured on the device first, and if the configuration is in a specified VRF, you have to delete all OSPF configurations under the specified VRF before configuring the command **set protocols ospf vrf network area**. Or if these configurations are in the default VRF, you have to delete all OSPF configurations of ***all*** VRFs on the device by using command **delete protocols ospf** before configuring **set protocols ospf network area**.

Example

- Enable OSPF for network 10.0.0.0/16 in VRF BLUE and specify area 1.1.1.1.

```
admin@XorPlus# set protocols ospf vrf BLUE network 10.0.0.0/16 area 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf passive-interface

Run the command **set protocols ospf passive-interface** to the set the specified layer 3 interface as passive OSPF interface. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify the VRF for this command to take effect in, if not specified the command affects the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Passive interfaces are part of the OSPF database but they do not send or receive OSPF LSAs and hence OSPF adjacencies are not formed on these interfaces.

To delete the configuration, run the command **delete protocols ospf passive-interface.**

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] passive-interface** <*interface*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] passive-interface** <*interface*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
passive-interface <interface>	Specify a L3-interfaces to set to passive mode.

Example

- Set interface *vlan20* to OSPF passive mode for OSPF instance ID 1 in the default VRF.

```
admin@XorPlus# set protocols ospf instance-id 1 passive-interface vlan20
admin@Xorplus# commit
```

set protocols ospf redistribute

Run the command **set protocol ospf redistribute** to redistribute routes of a specified type or protocol into OSPF. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF. You can optionally specify OSPF **metric** for the routes.

Run the command **delete protocol ospf redistribute** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|isis|rip|static|table** <*table-id*>**} [metric** <*metric*>**]**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|isis|rip|static|table** <*table-id*>**} [metric** <*metric*>**]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance. The value is a string.
bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
isis	Specify IS-IS routes for redistribution into OSPF.
rip	Specify RIP routes for redistribution into OSPF.
static	Specifies the static routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
metric <*metric*>	Optional. Specifies the route metric. The value is an integer that ranges from 0 to16777214.

Example

- Configure OSPF to redistribute BGP routes into OSPF in instance ID 1 with metric 5.

```
admin@XorPlus# set protocols ospf instance-id 1 redistribute bgp metric 5
admin@Xorplus# commit
```

set protocols ospf redistribute metric-type

Run the command **set protocols ospf redistribute metric-type** to specify metric type for OSPF route redistribution from other sources. There are two types of external routes, type 1 and type 2. A type 1 route has a metric that is the sum of the internal OSPF cost and the external redistributed cost. A type 2 route has a metric equal only to the redistributed cost. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. Optional VRF can be specified for the single instance OSPF to configure the metric type.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf redistribute metric-type** to delete this configuration.

Command Syntax

set protocol ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|static|table** <*table-id*>**} metric-type <1|2>**

delete protocol ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|static|table|table** <*table-id*>} **metric-type <1|2>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <vrf-name>	Optional. Specifies the name of the VRF for the OSPF instance.
protocol bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
static	Specifies the static routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
metric-type<1|2>	Specifies the OSPF external routes metric type. Metric type identifies how metric for the route is calculated.

Example

- Configure OSPF to redistribute BGP routes into OSPF with metric type 2.

```
admin@XorPlus# set protocols ospf instance-id 1 redistribute bgp metric-type 2
admin@Xorplus# commit
```

set protocols ospf redistribute route-map

Run the command **set protocols ospf redistribute route-map** to specify a route map to filter routes of different sources for redistribution into OSPF. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf redistribute route-map** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|static|table** <*table-id*>**} route-map** <*route-map*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] redistribute {bgp|connected|kernel|static|table** <*table-id*>**} route-map** <*route-map*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
static	Specifies the static routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
route-map <*route-map*>	Specifies the route map to filter routes before redistributing them into OSPF.

Example

- Configure OSPF to redistribute BGP routes into OSPF and filter routes using route map map1 for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 vrf BLUE redistribute bgp route-map map1
admin@Xorplus# commit
```

set protocols ospf router-id

Run the command **set protocols ospf router-id** to configure OSPF router ID. The router ID should be unique within the OSPF domain and is in the IPv4 dotted decimal format. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify OSFPv2 instance for a particular VRF. If VRF is not defined then OSPFv2 instance takes effect for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf route-id** to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] router-id** <*ipv4*>

delete protocols ospf [instance-id <*instance-id***>| vrf** <*vrf-name*>**] router-id** <*ipv4*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
router-id <*ipv4*>	Specify OSPF router ID. The value is in IPv4 dotted decimal format.

Example

- Configure OSPF router ID for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 router-id 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf summary-address

The **set protocols ospf summary-address** command summarizes the external routes with the matching address and mask. When advertising this route, its metric is set to the lowest cost path from among the routes that were summarized. This command can be used only on ASBR (Autonomous System Boundary Router).

Command Syntax

set protocols ospf [vrf <*vrf-name*>**] summary-address** <*prefix/mask*> [**no-advertise | tag** <*tag-value*>]

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
summary-address <*prefix/mask*>	Specifies summarizing routes matching IPv4 address and mask *prefix/mask*.
no-advertise	Optional. Do not advertise the aggregate route. Suppress routes that match the specified prefix/mask pair.
tag <*tag-value*>	Optional. Specify the tag for the aggregate route. The summary prefix will be advertised along with the tag value in External LSAs. The value is an integer that ranges from 0 to 4294967295.

Example

- The following commands configure OSPF route summarization for ASBR.

```
admin@Xorplus# set protocols ospf summary-address 10.2.0.0/16 tag 2
admin@Xorplus# commit
```

set protocols ospf timers lsa min-arrival

Run the command **set protocols ospf timers lsa min-arrival** to set the minimum delay in receiving a new version of an LSA. The value of this parameter is in milliseconds and ranges from 0 to 600000. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify a VRF for the OSPF instance. If a VRF is not specified here, the command will affect OSPF for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf timers lsa min-arrival** to remove this configuration and go back to default delay of 1000 milliseconds.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] timers lsa min-arrival** <*milliseconds*>

delete protocols ospf [instance-id <*instance-id***> | vrf** <vrf-name>**] timers lsa min-arrival** <*milliseconds*>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <vrf-name>	Optional. Specifies the name of the VRF for the OSPF instance.
min-arrival <*milliseconds*>	Specify the minimum delay in receiving a new LSA in milliseconds. The value is an integer that ranges from 0 to 600000.

Example

- Configure OSPF minimum delay to receive LSA to 2000 milliseconds for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 timers lsa min-arrival 2000
admin@Xorplus# commit
```

set protocols ospf timers throttle spf

Run the command **set protocols ospf timers throttle spf** to set the *initial delay,* the *initial hold time* and the *maximum hold time* between when the SPF is calculated and the event which triggered the calculation. These timers prevent the system from overburdening the CPU with frequent SPF calculations. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID. The optional parameter **vrf** can be used to specify the name of the VRF for this configuration to take effect on. If the VRF name is not specified, the command takes effect on OSPF for the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

Run the command **delete protocols ospf timers throttle spf** to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] timers throttle spf {delay**<*delay*> **| initial-holdtime**<*initial-hold-time*> **| maximum-holdtime**<*max-hold-time*>**}**

delete protocols ospf [instance-id <*instance-id***> | vrf** <*vrf-name*>**] timers throttle spf {**<*delay*> **|** <*initial-hold-time*> **|** <*max-hold-time*>**}**

Parameter

Parameter	Description
instance-id <*instance-id***>**	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
delay<*delay*>	Specifies the *initial delay*, the value ranges from 0 to 600000 milliseconds.
initial-holdtime<*initial-hold-time*>	Specifies the *initial hold time*, the value ranges from 0 to 600000 milliseconds.
maximum-holdtime<*max-hold-time*>	Specifies the *maximum hold time*, the value ranges from 0 to 600000 milliseconds.

Usage Guidelines

These three parameters are important fine tuning tools for OSPF. These timers are introduced to delay starting SFP calculations when a SPF-triggering event occurs. Frequent SPF calculations may incur heavy burden on the device resources such as CPU especially in large OSPF networks. The *delay* parameter specifies the delay in SPF calculation. This delay also applies to events occurring outside the *hold-time* of the previous SPF calculation. Two consecutive SPF calculations are always delayed by at least hold-time delay in milliseconds. The hold-time is initially set to the *initial hold-time* but its value is flexible and may be changed. If an event occurs within the hold-time of the previous SPF calculation, it results in increasing the hold-time by *initial hold-time.* If the flexible hold-time expires and no SPF triggering event occurs, the hold-time is reset to *initial hold-time*.

The example below sets the initial *delay* to 20ms, *initial hold-time* to 50ms and *maximum hold-time* to 5 seconds. This means that there will be a delay of 20ms between an SPF-triggering event and the commencement of the actual SPF calculation. The delay between two consecutive SPF calculations will be between 50ms and 5 seconds. If an SPF-triggering event occurs between the hold-time of the previous SPF calculation, the hold-time is increased by 50ms.

Example

- Configure OSPF SPF timers of initial delay time, minimum hold time and maximum hold time to 20, 50 and 5000ms respectively for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 timers throttle spf delay 20
admin@XorPlus# set protocols ospf instance-id 1 timers throttle spf initial-holdtime 50
admin@XorPlus# set protocols ospf instance-id 1 timers throttle spf maximum-holdtime 5000
admin@Xorplus# commit
```

set protocols ospf traceoption ism

Run the command **set protocols ospf traceoption** to enable debugging for OSPF Interface State Machine (ISM). Optionally, you can choose to enable three different types of logging information, **status**, for ISM status information, **events**, for ISM events, or **timers** to get logging for timer s related information. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

Run the command **delete protocols ospf traceoption ism** to delete this information.

Command Syntax

set protocols ospf [instance-id <*instance-id*>] traceoption ism <status | events | timers>

delete protocols ospf [instance-id <*instance-id*>] traceoption ism <status | events | timers>

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
ism <status | events | timers>	Specifies to enable ISM logging for either **status**, **events** or **timers**.

Example

- Enable OSPF ISM logging for status related information.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption ism status
admin@Xorplus# commit
```

set protocols ospf traceoption lsa

Run the command **set protocols ospf traceoption lsa** to enable logging of Link State Advertisement related messages. Three optional parameters, **generate, flooding, install,** or **refresh** can be used to specify logging for different types of LSA events. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run the command **delete protocols ospf traceoption lsa** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption lsa <generate | flooding | install | refresh>**

delete protocols ospf [instance-id <*instance-id***>] traceoption lsa <generate | flooding | install | refresh>**

Parameter

Parameter	Description
instance-id <*instance-id***>**	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
lsa <generate | flooding | install | refresh>	Specifies to enable LSA logging for **generate, flooding, install** or **refresh** events.

Example

- Enable OSPF LSA logging for flooding related information.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption lsa flooding
admin@Xorplus# commit
```

set protocols ospf traceoption nsm

Run the command **set protocols ospf traceoption nsm** to enable logging information of Network State Machine (NSM). Optional keywords **status, events** or **timers** can be used with this command to get log information on these specific NSM events. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run the command **delete protocols ospf traceoption nsm** to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption nsm <status | events | timers>**

delete protocols ospf [instance-id <*instance-id***>] traceoption nsm <status | events | timers>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
nsm <status | events | timers>	Optional. Specifies to enable NSM logging for **status**, **events** or **timers** events.

Example

- Enable OSPF NSM logging for status related information.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption NSM status
admin@Xorplus# commit
```

set protocols ospf traceoption packet

Run the command **set protocols ospf traceoption packet** to enable OSPF packet logging. Optional keywords can be used for logging information on specific packet types. These types are **hello, dd** (database description packets), **ls-request** (link-state request), **ls-update** (link-state update), **ls-ack** (link-state acknowledgement) and **all**. Optionally you can choose packet event type **send** or **receive**. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run **delete protocols ospf traceoption packet** the command to delete this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption packet {hello | dd | ls-request | ls-update | ls-ack | all } [send | recv | detail]**

delete protocols ospf [instance-id <*instance-id***>] traceoption packet {hello | dd | ls-request | ls-update | ls-ack | all } [send | recv | detail]**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
packet {hello|dd|ls-request|ls-update|ls-ack|all}	Specifies to enable OSPF logging for **hello,** database description **(dd),** link state request **(ls-request),** link state update **(ls-update),** link state acknowledgement **(ls-ack)** or **all**.
send|recv|detail	Optional. Specifies the send or receive direction and details.

Example

- Enable detailed OSPF hello packet logging.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption packet hello detail
admin@Xorplus# commit
```

set protocols ospf traceoption zebra

Run the command **set protocols ospf traceoption zebra** to enable OSPF zebra module related logging. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID.

Run the command **delete protocols ospf traceoption zebra** to remove this configuration from the database.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] traceoption zebra**

delete protocols ospf [instance-id <*instance-id***>] traceoption zebra**

Example

- Enable OSPF zebra module related logging for OSPF instance ID 1.

```
admin@XorPlus# set protocols ospf instance-id 1 traceoption zebra
admin@Xorplus# commit
```

set protocols ospf graceful-restart enable

Run the command **set protocols ospf graceful-restart enable** to enable the OSPF Graceful Restart (GR) capability on the restarting device. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. By default, OSPF GR capability is disabled.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart enable** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart enable <true | false>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) capability.
false	Disables OSPF Graceful Restart (GR) capability.

Usage Guidelines

To avoid traffic interruption and route oscillation caused by failover events, you can enable OSPF GR functionality on the restarting device by executing this command.

Example

- Enable OSPF Graceful Restart (GR) capability on the restarting device.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart enable true
admin@PICOS# commit
```

set protocols ospf capability opaque

Run the command **set protocols ospf capability opaque** to enable the capability to generate Opaque LSAs in the OSPF process, allowing the OSPF process to generate Opaque LSAs and receive them from neighboring devices. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf capability opaque** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] capability opaque**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] capability opaque**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Usage Guidelines

Opaque LSAs provide a generic mechanism for OSPF extensions, supporting the OSPF Graceful Restart (GR) feature through Type 9 LSAs. Therefore, before configuring OSPF GR, you must enable OSPF's Opaque LSA capability using this command.

Example

- Enable the capability to generate Opaque LSAs in the OSPF process.

```
admin@PICOS# set protocols ospf instance-id 1 capability opaque
admin@PICOS# commit
```

set protocols ospf graceful-restart grace-period

Run the command **set protocols ospf graceful-restart grace-period** to configure the maximum restart wait time. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart grace-period** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] grace-period <***grace-period***>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] grace-period**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
grace-period <*grace-period***>**	Specifies the maximum restart wait time, in seconds, advertised to neighbors. The value is an integer that ranges from 1 through 1800 seconds. The default value is 120 seconds.

Example

- Configure the maximum restart wait time.

```
admin@PICOS# set protocols ospf instance-id 1 grace-period 300
admin@PICOS# commit
```

set protocols ospf graceful-restart helper enable

Run the command **set protocols ospf graceful-restart helper enable** to enable the OSPF Graceful Restart (GR) Helper capability. By default, helper support is disabled for all neighbors. This config enables/disables helper support on this router for all neighbors. To enable/disable helper support for a specific neighbor, the router-id (A.B.C.D) has to be specified.

Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF. By default, OSPF GR Helper capability is disabled.

- If helper is enabled for specific neighbors, the global helper configuration for other neighbors will not take effect.
- Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper enable** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable <true | false>**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) Helper capability.
false	Disables OSPF Graceful Restart (GR) Helper capability.
router-id <*ipv4*>	Optional. Specifies the router-id (A.B.C.D) of the neighbor device to enable/disable helper support for a specific neighbor.

Example

- Enable OSPF Graceful Restart (GR) Helper capability.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper enable true
admin@PICOS# commit
```

set protocols ospf graceful-restart helper planned-only

Run the command **set protocols ospf graceful-restart helper planned-only** to enable the OSPF Graceful Restart (GR) Helper to support only Planned Graceful Restart. By default, the device supports both Planned Graceful Restart and Unplanned Graceful Restart. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper planned-only** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper planned-only**

delete protocols ospf [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper planned-only**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Example

- Enable the OSPF Graceful Restart (GR) Helper to support only Planned Graceful Restart.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper planned-only
admin@PICOS# commit
```

set protocols ospf graceful-restart helper strict-lsa-checking

Run the command **set protocols ospf graceful-restart helper strict-lsa-checking** to configure strict LSA checking on the Helper Router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. Strict LSA checking is enabled by default.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper strict-lsa-checking** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper strict-lsa-checking enable <true | false>**

delete protocols ospf [instance-id <*instance-id***>] [vrf <***vrf-name***>] graceful-restart helper strict-lsa-checking enable <true | false>**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables strict LSA checking.
false	Disables strict LSA checking.

Usage Guidelines

The strict LSA checking feature allows a helper router to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. You can enable strict LSA checking on an OSPF helper to have the router terminate graceful restart when there is a change to an LSA that would be flooded to the restarting router. This feature takes effect only when the router is in helper mode.

Example

- Enable strict LSA checking on the Helper Router.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper strict-lsa-checking enable true
admin@PICOS# commit
```

set protocols ospf graceful-restart helper supported-grace-time

Run the command **set protocols ospf graceful-restart helper supported-grace-time** to configure the period for Graceful Restart on the Helper router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv2 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf graceful-restart helper supported-grace-time** can be used to remove this configuration.

Command Syntax

set protocols ospf [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper supported-grace-time <***supported-grace-time***>**

delete protocols ospf [instance-id <*instance-id***>] [vrf <***vrf-name***>] graceful-restart helper supported-grace-time**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
supported-grace-time <*supported-grace-time***>**	Specifies the period for Graceful Restart on the Helper router. The value is an integer that ranges from 10 through 1800 seconds. There is no default value.

Example

- Configure the period for Graceful Restart on the Helper router.

```
admin@PICOS# set protocols ospf instance-id 1 graceful-restart helper supported-grace-time 300
admin@PICOS# commit
```

run graceful-restart prepare ospf

The **run graceful-restart prepare ospf** command is a operational command that the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain, informing its neighbors about its restarting process and the estimated time for the restart to complete. These LSAs are Type 9 LSAs and are flooded throughout the OSPF domain.

The OSPF protocol should be restarted during the grace period, otherwise the graceful restart will fail.

To perform a graceful shutdown, this operational command needs to be issued before restarting the OSPF protocol.

- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

Command Syntax

run graceful-restart prepare ospf

Parameters

None.

Example

- Configure to let the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain.

```
admin@Xorplus# run graceful-restart prepare ospf
```

run show ospf graceful-restart helper

Run the command **run show ospf graceful-restart helper** to display the Graceful Restart Helper details including helper config changes.

Command Syntax

run show ospf [**instance-id <***instance-id***>**][**vrf<***vrf-name***>**] **graceful-restart helper [detail]**

Parameters

Parameter	Description
instance-id <*instance-id*>	Optional. Specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the VRF name, the value is a string.

Example

- Display the Graceful Restart Helper details including helper config changes.

```
admin@PICOS# run show ospf graceful-restart helper
OSPF Router with ID (2.2.2.2)
 Graceful restart helper support enabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
```

OSPFv3 Command Reference

- set protocols ospf6 area
- set protocols ospf6 area range
- set protocols ospf6 area stub
- set protocols ospf6 area stub no-summary
- set protocols ospf6 auto-cost reference-bandwidth
- set protocols ospf6 distance
- set protocols ospf6 distance-ospf6
- set protocols ospf6 interface area
- set protocols ospf6 interface cost
- set protocols ospf6 interface dead-interval
- set protocols ospf6 interface hello-interval
- set protocols ospf6 interface ifmtu
- set protocols ospf6 interface mtu-ignore
- set protocols ospf6 interface network
- set protocols ospf6 interface passive
- set protocols ospf6 interface priority
- set protocols ospf6 interface retransmit-interval
- set protocols ospf6 interface transmit-delay
- set protocols ospf6 log-adjacency-changes
- set protocols ospf6 redistribute
- set protocols ospf6 router-id
- set protocols ospf6 stub-router administrative
- set protocols ospf6 timers lsa min-arrival
- set protocols ospf6 timers throttle spf
- set protocols ospf6 traceoption
- set protocols ospf6 traceoption border-routers
- set protocols ospf6 traceoption lsa
- set protocols ospf6 traceoption message
- set protocols ospf6 traceoption neighbor
- set protocols ospf6 traceoption route
- set protocols ospf6 traceoption spf
- set protocols ospf6 traceoption zebra
- set protocols ospf6 graceful-restart enable
- set protocols ospf6 capability opaque
- set protocols ospf6 graceful-restart grace-period
- set protocols ospf6 graceful-restart helper enable
- set protocols ospf6 graceful-restart helper planned-only
- set protocols ospf6 graceful-restart helper lsa-checking-disable
- set protocols ospf6 graceful-restart helper supported-grace-time
- run graceful-restart prepare ospf6
- run show ospf6 graceful-restart helper

set protocols ospf6 area

Use the command **set protocols ospf6 area** to configure area for the OSPFv3 instance.

Run the command **delete protocols ospf6 area** to delete this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **area{<***ipv4***> | <***area-id***>}**

delete protocols ospf6 [**vrf** <*vrf-name*>] **area{<***ipv4***> | <***area-id***>}**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area{<*ipv4***> | <***area-id***>}**	Specifies the area for OSPFv3, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Example

- This example configures the OSPFv3 area ID to 0.0.0.0.

```
admin@XorPlus# set protocols ospf6 area 0.0.0.0
```

set protocols ospf6 area range

Run the command **set protocols ospf6 area range** to configure a summary route for all the routes in that range. The range parameter is used on the ABRs for the purpose of managing the size of the routing table.

Run the command **delete protocols ospf6 area range** to remove this configuration from the switch.

Command Syntax

set protocol ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} range <***ipv6/prefixlen***>** [**advertise <true | false>** | **cost** <*cost*>]

delete protocol ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} range <***ipv6/prefixlen***>** [**advertise <true | false>** | **cost** <*cost*>]

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area {<*ipv4*>| <*area-id***>}**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
range <*ipv6/prefixlen***>**	Specifies the range parameter, the value is in IPv6/prefix length format.
advertise <true | false>	Optional. Determines whether to advertise the summarized route or not. The value could be **true** or **false**. • **true**: Advertise the summarized route. • **false**: Do not advertise the summarized route. By default, the summarized route is advertised.
cost <*cost***>**	Optional. Specifies the cost of the summarized route. The value is an integer that ranges from 0 to 16777215.

Example

- This example creates a summary route for all the routes in the range 2001::/64.

```
admin@XorPlus# set protocols ospf6 area 0.0.0.0 range 2001::/64
```

set protocols ospf6 area stub

Run the command **set protocols ospf6 area stub** to configure a stub area for the OSPFv3 instance.

Run the command **delete protocols ospf6 area stub** to delete this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4***>|<***area-id***>} stub**

delete protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4***>|<***area-id***>} stub**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area {<*ipv4***>|<***area-id***>}**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Example

- This example configures area 1.1.1.1 as a stub area of the OSPFv3 instance in the default VRF.

```
admin@XorPlus# set protocols ospf6 area 1.1.1.1 stub
```

set protocols ospf6 area stub no-summary

Run the command **set protocols ospf6 area stub no-summary** to configure a stub area with no-summary option. The no-summary option disallows the injection of summary routes into an area and thus makes the area a *totally-stubby* area.

Run the command **delete protocols ospf6 area stub no-summary** to delete this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} stub no-summary**

delete protocols ospf6 [**vrf** <*vrf-name*>] **area {<***ipv4*>|<*area-id***>} stub no-summary**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
area {<*ipv4*>|<*area-id***>}**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Example

- This example configures area 1.1.1.1 as a totally-stubby area of the OSPFv3 instance in the default VRF.

```
admin@XorPlus# set protocols ospf6 area 1.1.1.1 stub no-summary
```

set protocols ospf6 auto-cost reference-bandwidth

Run the command **set protocols ospf6 auto-cost reference-bandwidth** to set the reference bandwidth for automatic route cost calculation. The reference bandwidth specified here is considered equivalent to OSPF cost of 1. The default bandwidth is 100Mbits/s, that is, a link with bandwidth of 100Mbits/s or higher is considered to have a cost of 1. Cost of links with lower bandwidth will be calculated with reference to this bandwidth value.

Note that this configuration must be consistent within the OSPF domain.

Run the command **delete protocols ospf6 auto-cost reference-bandwidth** to delete this configuration

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **auto-cost reference-bandwidth**<*ref-bandwidth*>

delete protocols ospf6 [**vrf** <*vrf-name*>] **auto-cost reference-bandwidth**<*ref-bandwidth*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
reference-bandwidth <*ref-bandwidth*>	Specifies the reference bandwidth. The value is an integer that ranges from 1 to 4294967.

Example

- Configure the OSPFv3 reference bandwidth to 500000.

```
admin@XorPlus# set protocols ospf6 auto-cost reference-bandwidth 500000
admin@Xorplus# commit
Commit Ok.
Save done
```

set protocols ospf6 distance

The command **set protocols ospf6 distance** configures the administrative distance for an entire group of OSPFv3 routes.

Run the command **delete protocols ospf6 distance** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **distance <***distance***>**

delete protocols ospf6 [**vrf** <*vrf-name*>] **distance** <*distance*>

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
distance <*distance***>**	Specifies the administrative distance, the value is an integer that ranges from 1 to 255

Example

- This example configures the administration distance of OSPF routes to 140.

```
admin@XorPlus# set protocols ospf6 distance 140
```

set protocols ospf6 distance-ospf6

Run the command **set protocols ospf6 distance-ospf6** to configure the administrative distance for intra-area, inter-area and external routes.

Run the command **delete protocols ospf6 distance-ospf6** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **distance-ospf6 {intra-area <***distance***> | inter-area <***distance***> | external <***distance***>}**

delete protocols ospf6 [**vrf** <*vrf-name*>] **distance-ospf6 {intra-area <***distance***> | inter-area <***distance***> | external <***distance***>}**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
intra-area <*distance***>**	Specifies the administrative distance for intra-area routes. The values is an integer that ranges from 1 to 255.
inter-area <*distance***>**	Specifies the administrative distance for inter-area routes. The values is an integer that ranges from 1 to 255.
external <*distance***>**	Specifies the administrative distance for external routes. The values is an integer that ranges from 1 to 255.

Example

- This example configures the administrative distance of inter-area routes and intra-area routes to 200 and sets the administrative distance for external routes to 250.

```
admin@XorPlus# set protocols ospf6 distance ospf6 intra-area 200
admin@XorPlus# set protocols ospf6 distance-ospf6 inter-area 200
admin@XorPlus# set protocols ospf6 distance-ospf6 external 250
admin@XorPlus# commit
```

set protocols ospf6 interface area

Run the command **set protocols ospf6 interface area** to enable OSPFv3 on a specific interface and map that interface to an area.

Run the command **delete protocols ospf6 interface** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **area <***ipv4***>**

delete protocols ospf6 interface <*interface-name***> area <***ipv4***>**

Parameters

Parameter	Description
area <*ipv4***>**	Specifies the area for OSPFv3, the value is in IPv4 dotted decimal format.
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Usage Guidelines

You can add the L3 interface to a specified VRF to specify the VRF for the OSPFv3 instance. If L3 VLAN interface/loopback interface is not added to a specified VRF, then the command takes effect in the default VRF.

The following commands add the L3 VLAN interface to a specified VRF and specify the VRF for the OSPFv3 instance.

```
admin@XorPlus# set l3-interface vlan-interface vlan100 vrf "vrf1"
admin@XorPlus# set protocols ospf6 interface vlan100 area 0.0.0.0
```

Example

- This example enable OSPFv3 on L3 VLAN interface vlan100 and bind the interface to area 0.0.0.0.

```
admin@XorPlus# set protocols ospf6 interface vlan100 area 0.0.0.0
```

set protocols ospf6 interface cost

Run the command **set protocols ospf6 interface cost** to set the OSPF link cost for the specified interface. The cost value is set to router-LSA's metric field and used for SPF calculation. Changing the interface cost causes the OSPF to run the SPF and reissue LSAs.

Run the command **delete protocols ospf6 interface cost** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **cost** <*1-65535*>

delete protocols ospf6 interface <*interface-name*> **cost**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
cost <*1-65535*>	Specifies the link cost, the value is an integer in the range of 1 to 65535.

Example

- Set the OSPFv3 interface vlan200 cost to 5.

```
admin@XorPlus# set protocols ospf6 interface vlan200 cost 5
admin@Xorplus# commit
```

set protocols ospf6 interface dead-interval

Run the command **set protocols ospf6 interface dead-interval** to configure the OSPF neighbor router dead interval in seconds. This value must be the same on all routers in the OSPF domain.

Run the command **delete protocols ospf6 interface dead-interval** to remove this configuration and revert to the default value which is 40 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **dead-interval** <*1-65535*>

delete protocols ospf interface <*interface-name*> **dead-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
dead-interval <*1-65535*>	Specifies the OSPFv3 neighbor dead interval in seconds. The value ranges from 1 to 65535. The default interval is 40 seconds.

Example

- Configure the OSPFv3 neighbor dead interval to 60 seconds.

```
admin@XorPlus# set protocols ospf6 interface vlan200 dead-interval 60
admin@Xorplus# commit
```

set protocols ospf6 interface hello-interval

Run the command **set protocols ospf6 interface hello-interval** to set the OSPF hello interval on the specified interface. Hello packets will be sent every **hello-interval** of time. The default value is 10 seconds.

Run the command **delete protocols ospf interface hello-interval** to remove this configuration and revert back to the default 10 seconds.

Command Syntax

set protocols ospf interface <*interface-name*> **hello-interval** <*1-65535*>

delete protocols ospf interface <*interface-name*> **hello-interval** <*1-65535*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
hello-interval <*1-65535*>	Specifies the hello interval in seconds. The value ranges from 1 to 65535. The default value is 10 seconds.

Example

- Configure the hello interval to 60 seconds on interface vlan200.

```
admin@XorPlus# set protocols ospf6 interface vlan200 hello-interval 60
admin@Xorplus# commit
```

set protocols ospf6 interface ifmtu

Run the command **set protocols ospf6 interface ifmtu** to configure the OSPFv3 interface MTU.

Run the command **delete protocols ospf6 interface ifmtu** to delete this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name***> ifmtu <***1-65535***>**

delete protocols ospf6 interface <*interface-name***> ifmtu <***1-65535***>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
ifmtu <*1-65535***>**	Specifies the OSPFv3 interface MTU, the value is an integer that ranges from 1 to 65535.

Example

- Set the OSPFv3 interface MTU to 1400.

```
admin@XorPlus# set protocols ospf6 interface vlan200 ifmtu 1400
admin@Xorplus# commit
```

set protocols ospf6 interface mtu-ignore

Run the command **set protocols ospf6 interface mtu-ignore** to disable ignore MTU mismatch detection on this interface.

Run the command **delete protocols ospf6 interface mtu-ignore** to delete this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **mtu-ignore**

protocols ospf6 interface <*interface-name*> **mtu-ignore**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Example

- This example configures the MTU mismatch detection on the interface *vlan10*.

```
admin@XorPlus# set protocols ospf6 interface vlan10 mtu-ignore
admin@XorPlus# commit
```

set protocols ospf6 interface network

Run the command **set protocols ospf6 interface network** to enable OSPF on an interface and specify a network type. Enabling OSPF on an interface allows the interface to send and receive LSAs. Two different network types can be specified here namely, **broadcast** and **point-to-point**.

To delete this configuration, run the command **delete protocols ospf interface network**

Command Syntax

set protocols ospf interface <*interface-name*> **network <broadcast|point-to-point>**

delete protocols ospf interface <*interface-name*> **network <broadcast|point-to-point>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
broadcast	Specifies the OSPF broadcast multi-access network.
point-to-point	Specifies the OSPF point-to-point network.

Example

- Enable OSPFv3 on interface vlan200 and specify network type as point-to-point.

```
admin@XorPlus# set protocols ospf interface vlan200 network point-to-point
admin@Xorplus# commit
```

set protocols ospf6 interface passive

Run the command **set protocols ospf6 interface passive** to identify a specific interface as OSPFv3 passive interface. Passive interfaces are part of OSPFv3 database but they do not send or receive OSPF LSAs. OSPFv3 does not try to form adjacency relationship with peers on these interfaces.

Run the command **delete protocols ospf6 interface passive** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name***> passive**

delete protocols ospf6 interface <*interface-name***> passive**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.

Example

- Set the interface vlan200 as OSPFv3 passive interface.

```
admin@XorPlus# set protocols ospf6 interface vlan200 passive
admin@Xorplus# commit
```

set protocols ospf6 interface priority

Run the command **set protocols ospf6 interface priority** to set the interface's router priority. The default value is 1.

Run the command **delete protocols ospf6 interface priority** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name***> priority <***priority***>**

delete protocols ospf6 interface <*interface-name*> **priority <***priority***>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
priority <*priority***>**	Specifies the interface's router priority, the value is an integer that ranges from 0 to 255. The default value is 1.

Example

- Set the interface vlan200 router priority to 2.

```
admin@XorPlus# set protocols ospf6 interface vlan200 priority 2
admin@Xorplus# commit
```

set protocols ospf6 interface retransmit-interval

Run the command **set protocols ospf6 interface retransmit-interval** to configure the LSA retransmit interval for adjacencies belonging to the OSPFv3 interface for lost LSAs.

Run the command **delete protocols ospf6 interface retransmit-interval** to delete this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **retransmit-interval <***seconds***>**

delete protocols ospf6 interface <*interface-name*> **retransmit-interval <***seconds***>**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
retransmit-interval <*seconds***>**	Specifies the LSA retransmit interval for the OSPFv3 interface in seconds. The value is an integer that ranges from 1 to 65535.

Example

- Set the retransmit interval for lost LSAs for the OSPFv3 interface to 10 seconds.

```
admin@XorPlus# set protocols ospf6 interface vlan200 retransmit-interval 10
admin@Xorplus# commit
```

set protocols ospf6 interface transmit-delay

Run the command **set protocols ospf6 interface transmit-delay** to set the estimated time needed to send an OSPFv3 LSA update packet.

Run the command **delete protocols ospf6 interface transmit-delay** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 interface *<interface-name>* **transmit-delay <***seconds***>**

delete protocols ospf6 interface *<interface-name>* **transmit-delay <***seconds***>**

Parameter

Parameter	Description
interface *<interface-name>*	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
transmit-delay <*seconds***>**	Specifies the transmit delay in seconds, the value is an integer that ranges from 1 to 3600.

Example

- Set the OSPFv3 interface transmit delay to 20 seconds.

```
admin@XorPlus# set protocols ospf6 interface vlan200 transmit-delay 20
admin@Xorplus# commit
```

set protocols ospf6 log-adjacency-changes

Run the command **set protocols ospf6 log-adjacency-changes** to enable logging OSPFv3 adjacency changes. The optional parameter **detail** can be used to log all adjacency status changes. Without the **detail** keyword, only the adjacency changes to full or regression are logged.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **log-adjacency-changes [detail]**

delete protocols ospf6 [**vrf** <*vrf-name*>] **log-adjacency-changes [detail]**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.

Example

- This example enables all OSPFv3 adjacency changes logging.

```
admin@XorPlus# set protocols ospf6 log-adjacency-changes detail
admin@XorPlus# commit
```

set protocols ospf6 redistribute

Run the command **set protocols ospf6 redistribute** to redistribute routes from other sources and protocols through OSPFv3. Users can add the **route-map** parameter to include a route map to filter routes before redistribution.

To delete this configuration, run the command **delete protocols ospf6 redistribute.**

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **redistribute {bgp|connected|kernel|isis|ripng|static|table} [route-map<***route-map***>]**

delete protocols ospf6 [**vrf** <*vrf-name*>] **redistribute {bgp|connected|kernel|isis|ripng|static|table} [route-map<***route-map***>]**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
bgp	Specify BGP routes for redistribution into OSPF.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
isis	Specify IS-IS routes for redistribution into OSPF.
ripng	Specify RIPng routes for redistribution into OSPF.
static	Specifies the static routes for redistribution.
table	Redistribute routes from table.
route-map<*route-map***>**	Optional. Specifies a route map for filtering routes before redistribution.

Example

- Configure OSPFv3 to redistribute BGP routes into OSPFv3 and apply route-map *map1* for route filtering.

```
admin@XorPlus# set protocols ospf6 redistribute bgp route-map map1
admin@Xorplus# commit
```

set protocols ospf6 router-id

Run the command **set protocols ospf6 router-id** to configure OSPFv3 router ID. The router ID should be unique within the OSPF domain and is in the IPv4 dotted decimal format.

Run the command **delete protocols ospf route-id** to delete this configuration.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **router-id** <ipv4>

delete protocols ospf6 [**vrf** <*vrf-name*>] **router-id** <ipv4>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
router-id <ipv4>	Specify OSPFv3 router ID. The value is in IPv4 dotted decimal format.

Example

- Configure OSPFv3 router ID.

```
admin@XorPlus# set protocols ospf6 router-id 1.1.1.1
admin@Xorplus# commit
```

set protocols ospf6 stub-router administrative

Run the command **set protocols ospf6 stub-router administrative** to make a router a stub router for indefinite period of time.

Run the command **delete protocols ospf6 stub-router administrative** to delete this configuration.

Command Syntax

set protocol ospf6 [**vrf** <*vrf-name*>] **stub-router administrative**

delete protocol ospf6 [**vrf** <*vrf-name*>] **stub-router administrative**

Parameters

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.

Example

- This example configures OSPF stub router for an indefinite period of time.

```
admin@XorPlus# set protocols ospf6 stub-router administrative
admin@Xorplus# commit
```

set protocols ospf6 timers lsa min-arrival

Run the command **set protocols ospf6 timers lsa min-arrival** to set the minimum delay in receiving a new version of an LSA. The value of this parameter is in milliseconds and ranges from 0 to 600000.

Run the command **delete protocols ospf6 timers lsa min-arrival** to remove this configuration and go back to default delay of 1000 milliseconds.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **timers lsa min-arrival** <*milliseconds*>

delete protocols ospf6 [**vrf** <*vrf-name*>] **timers lsa min-arrival** <*milliseconds*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
min-arrival <*milliseconds*>	Specify the minimum delay in receiving a new LSA in milliseconds. The value is an integer that ranges from 0 to 600000.

Example

- Configure OSPFv3 minimum delay to receive LSA to 2000 milliseconds.

```
admin@XorPlus# set protocols ospf6 timers lsa min-arrival 2000
admin@Xorplus# commit
```

set protocols ospf6 timers throttle spf

Run the command **set protocols ospf6 timers throttle spf** to set the initial *delay,* the *initial hold-time* and the *maximum hold-time* between when the SPF is calculated and the event which triggered the calculation. These timers prevents the system from overburdening the CPU with frequent SPF calculations.

Run the command **delete protocols ospf timers throttle spf** to delete this configuration.

Command Syntax

set protocols ospf6 [**vrf** <*vrf-name*>] **timers throttle spf {delay<***delay***> | initial-holdtime<***nitial-hold-time***> | maximum-holdtime<***max-hold-time***>}**

delete protocols ospf6 [**vrf** <*vrf-name*>] **timers throttle spf {delay**<*delay*> **| initial-holdtime**<*delay*> **| maximum-holdtime**<*max-hold-time*>**}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPFv3 instance.
delay<*delay***>**	Specifies the *initial delay*, the value ranges from 0 to 600000 milliseconds.
initial-holdtime<*nitial-hold-time***>**	Specifies the *initial hold time*, the value ranges from 0 to 600000 milliseconds.
maximum-holdtime<*max-hold-time*>	Specifies the *maximum hold time*, the value ranges from 0 to 600000 milliseconds.

Usage Guidelines

These three parameters are important fine tuning tools for OSPFv3. These timers are introduced to delay starting SFP calculations when a SPF-triggering event occurs. Frequent SPF calculations may incur heavy burden on the device resources such as CPU especially in large OSPFv3 networks. The *delay* parameter specifies the delay in SPF calculation. This delay also applies to events occurring outside the *hold-time* of the previous SPF calculation. Two consecutive SPF calculations are always delayed by at least hold-time delay in milliseconds. The hold-time is initially set to the *initial hold-time* but its value is flexible and may be changed. If an event occurs within the hold-time of the previous SPF calculation, it results in increasing the hold-time by *initial hold-time.* If the flexible hold-time expires and no SPF triggering event occurs, the hold-time is reset to *initial hold-time.*

The example below sets the initial *delay* to 20ms, *initial hold-time* to 50ms and *maximum hold-time* to 5 seconds. This means that there will be a delay of 20ms between an SPF-triggering event and the commencement of the actual SPF calculation. The delay between two consecutive SPF calculations will be between 50ms and 5 seconds. If an SPF-triggering event occurs between the hold-time of the previous SPF calculation, the hold-time is increased by 50ms.

Example

- Configure OSPFv3 SPF times of initial delay, initial hold-time and maximum hold-time to 20ms, 50ms and 5000ms respectively.

```
admin@XorPlus# set protocols ospf6 timers throttle spf delay 20
admin@XorPlus# set protocols ospf6 timers throttle spf initial-holdtime 50
admin@XorPlus# set protocols ospf6 timers throttle spf maximum-holdtime 5000
admin@Xorplus# commit
```

set protocols ospf6 traceoption

Run the command **set protocols ospf6 traceoption** to enable debugging for the OSPFv3 instance. Debugging information can be enabled for different features of OSPFv3 such as **abr** (Area Border Router), **asbr** (Autonomous System Border Router), **flooding** or **interface**.

To remove the configuration, run the command **delete protocols ospf6 traceoption.**

Command Syntax

set protocols ospf6 traceoption <abr | asbr | flooding | interface>

delete protocols ospf6 traceoption <abr | asbr | flooding | interface>

Parameters

Parameter	Description
abr	Choose this parameter to enable debugging related to OSPFv3 ABR events.
asbr	Choose this parameter to enable debugging related to OSPFv3 ASBR events.
flooding	Choose this parameter to enable debugging related to OSPFv3 flooding events.
interface	Choose this parameter to enable debugging related to OSPFv3 interface events.

Example

- This example enables OSPFv3 debugging for flooding events.

```
admin@XorPlus# set protocols ospf6 traceoption flooding
```

set protocols ospf6 traceoption border-routers

Run the command **set protocols ospf6 traceoption border-routers** to enable or disable border routers relation debug information. Optional parameters **area-id** or **router-id** can be used to specify the area ID or router ID for which to enable/disable debug information.

Run the command **delete protocols ospf6 traceoption border-routers** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption border-routers [area-id <*ipv4***> | router-id <***ipv4***>]**

delete protocol ospf6 traceoption border-routers [area-id <*ipv4***> | router-id <***ipv4***>]**

Parameters

Parameter	Description
area <*ipv4***>**	Specifies the area ID for the OSPFv3 instance. The value is either in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.
router-id <*ipv4***>**	Specifies the router ID, the value is in IPv4 dotted decimal format.

Example

- This example enables border routers debug information for area 0.0.0.0.

```
admin@XorPlus# set protocols ospf6 border-routers area-id 0.0.0.0
```

set protocols ospf6 traceoption lsa

Run the command **set protocols ospf6 traceoption lsa** to enable debug information related to Link State Advertisement. The user can choose different components of OSPFv3 while enabling or disabling LSA related debug info such as **router**, **network** etc.

To remove this configuration, run the command **delete protocols traceoption lsa**

Command Syntax

set protocols ospf6 traceoption lsa <router | network | inter-prefix | inter-router | as-external | link | intra-prefix | unknown> [originate | examine | flooding]

delete protocol ospf6 traceoption lsa <router | network | inter-prefix | inter-router | as-external | link | intra-prefix | unknown> [originate | examine | flooding]

Example

- This example enables LSA debugging for routers.

```
admin@XorPlus# set protocols ospf6 lsa router
```

set protocols ospf6 traceoption message

Run the command **set protocols ospf6 traceoption message** to enable or disable OSPFv3 messages related debugging. The user can choose from a range of different packet types while enablling/disabling debug information such as unknow packets, hello packets etc. Optionally, the user can choose between packets sent or received for debugging.

Run the command **delete protocols ospf6 traceoption message** to delete this configuration.

Command Syntax

set protocols ospf6 traceoption message <unknown | hello | dbdesc | lsreq | lsupdate | lsack | all> [send|recv]

delete protocols ospf6 traceoption message <unknown | hello | dbdesc | lsreq | lsupdate | lsack | all> [send|recv]

Parameters

Parameter	Description
unknown	Specifies unknow packets.
hello	Specifies OSPFv3 hello packets.
dbdesc	Specifies OSPFv3 database description packets.
lsreq	Specifies Link State Request packets.
lsupdate	Specifies Link State Update packets.
lsack	Specifies Link State ACK packets.
all	Specifies debugging of all packets.
send	Optional. Specifies packets sent.
recv	Optional. Specifies packets received.

Example

- This example enables the OSPFv3 received link state update packet debugging.

```
admin@XorPlus# set protocols ospf6 traceoption lsupdate recv
```

set protocols ospf6 traceoption neighbor

Run the command **set protocols ospf6 traceoption neighbor** to enable OSPFv3 neighbor related debugging. The user can choose between **state** or **event** related debugging information or can choose **all** to enable all debugging related to neighbor state change.

Run the command **delete protocols ospf6 traceoption neighbor** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption neighbor <state | event | all>

delete protocols ospf6 traceoption neighbor <state | event | all>

Example

- This example enables OSPFv3 neighbor state related debugging.

```
admin@XorPlus# set protocols ospf6 neighbor state
```

set protocols ospf6 traceoption route

Run the command **set protocols ospf6 traceoption route** to enable route related debugging. The user can choose between different types of route debugging options such as **table, inter-area** etc to get debugging related to these specific events. Its important to note that inter-area routes are those routes which are created from Router LSAs and Network LSAs. Also to get information about memory usage of the routes, the user can choose the option **memory.** To get route debugging for the routing table then the user can choose the option **table.**

Run the command **delete protocols ospf6 traceoption route** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption route {table|intra-area|inter-area|memory}

delete protocol ospf6 traceoption route {table|intra-area|inter-area|memory}

Example

- This example configures OSPFv3 debugging for inter-area routes.

```
admin@XorPlus# set protocols ospf6 traceoption inter-area
```

set protocols ospf6 traceoption spf

Run the command **set protocols ospf6 traceoption spf** to enable the OSPFv3 SPF related debugging. The user can append **database** or **process** or **time** to enable specific SPF debugging. The **database** option enables logging of the number of LSAs at SPF calculation time. The **process** keyword will enable detailed debugging of the entire SPF process. The **time** option enables debugging of time taken by SPF calculation.

Run the command **delete protocols ospf6 traceoption spf** to delete this configuration.

Command Syntax

set protocols ospf6 traceoption spf <database | process | time>

delete protocols ospf6 traceoption spf <database | process | time>

Example

- This example configures the OSPFv3 SPF database related debugging.

```
admin@XorPlus# set protocols ospf6 traceoption spf database
```

set protocols ospf6 traceoption zebra

Run the command **set protocols ospf6 traceoption zebra** to configure OSPFv3 zebra module related debugging. Use the arguments **send, recv** or **all** to specify debugging for either packets sent, received or both.

Run the command **delete protocols ospf6 traceoption zebra** to remove this configuration from the switch.

Command Syntax

set protocols ospf6 traceoption zebra <send | recv | all>

delete protocols ospf6 traceoption zebra <send | recv | all>

Example

- This example configures the OSPFv3 zebra module packet debugging for packets received.

```
admin@XorPlus# set protocols ospf6 traceoption zebra received
```

set protocols ospf6 graceful-restart enable

Run the command **set protocols ospf6 graceful-restart enable** to enable the OSPFv3 Graceful Restart (GR) capability on the restarting device. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. By default, OSPF GR capability is disabled.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPFv3 are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart enable** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart enable <true | false>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) capability.
false	Disables OSPF Graceful Restart (GR) capability.

Usage Guidelines

To avoid traffic interruption and route oscillation caused by failover events, you can enable OSPFv3 GR functionality on the restarting device by executing this command.

Example

- Enable OSPFv3 Graceful Restart (GR) capability on the restarting device.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart enable true
admin@PICOS# commit
```

set protocols ospf6 capability opaque

Run the command **set protocols ospf6 capability opaque** to enable the capability to generate Opaque LSAs in the OSPFv3 process, allowing the OSPFv3 process to generate Opaque LSAs and receive them from neighboring devices. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPFv3 are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 capability opaque** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] capability opaque**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] capability opaque**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Usage Guidelines

Opaque LSAs provide a generic mechanism for OSPFv3 extensions, supporting the OSPFv3 Graceful Restart (GR) feature through Type 9 LSAs. Therefore, before configuring OSPFv3 GR, you must enable OSPF's Opaque LSA capability using this command.

Example

- Enable the capability to generate Opaque LSAs in the OSPFv3 process.

```
admin@PICOS# set protocols ospf6 instance-id 1 capability opaque
admin@PICOS# commit
```

set protocols ospf6 graceful-restart grace-period

Run the command **set protocols ospf6 graceful-restart grace-period** to configure the maximum restart wait time. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPFv3 are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart grace-period** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] grace-period <***grace-period***>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] grace-period**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
grace-period <*grace-period***>**	Specifies the maximum restart wait time, in seconds, advertised to neighbors. The value is an integer that ranges from 1 through 1800 seconds. The default value is 120 seconds.

Example

- Configure the maximum restart wait time.

```
admin@PICOS# set protocols ospf6 instance-id 1 grace-period 300
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper enable

Run the command **set protocols ospf6 graceful-restart helper enable** to enable the OSPFv3 Graceful Restart (GR) Helper capability. By default, helper support is disabled for all neighbors. This config enables/disables helper support on this router for all neighbors. To enable/disable helper support for a specific neighbor, the router-id (A.B.C.D) has to be specified.

Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF. By default, OSPF GR Helper capability is disabled.

- If helper is enabled for specific neighbors, the global helper configuration for other neighbors will not take effect.
- Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper enable** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable <true | false>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper** [**router-id** <*ipv4*>] **enable**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
true	Enables OSPF Graceful Restart (GR) Helper capability.
false	Disables OSPF Graceful Restart (GR) Helper capability.
router-id <*ipv4*>	Optional. Specifies the router-id (A.B.C.D) of the neighbor device to enable/disable helper support for a specific neighbor.

Example

- Enable OSPFv3 Graceful Restart (GR) Helper capability.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper enable true
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper planned-only

Run the command **set protocols ospf6 graceful-restart helper planned-only** to enable the OSPFv3 Graceful Restart (GR) Helper to support only Planned Graceful Restart. By default, the device supports both Planned Graceful Restart and Unplanned Graceful Restart. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper planned-only** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf**<*vrf-name*>**] graceful-restart helper planned-only**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper planned-only**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Example

- Enable the OSPFv3 Graceful Restart (GR) Helper to support only Planned Graceful Restart.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper planned-only
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper lsa-checking-disable

Run the command **set protocols ospf6 graceful-restart helper lsa-checking-disable** to configure strict LSA checking on the Helper Router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF. OSPFv3 strict LSA checking is disabled by default.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper lsa-checking-disable** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper strict-lsa-checking**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper strict-lsa-checking**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.

Usage Guidelines

The strict LSA checking feature allows a helper router to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. You can enable strict LSA checking on an OSPF helper to have the router terminate graceful restart when there is a change to an LSA that would be flooded to the restarting router. This feature takes effect only when the router is in helper mode.

Example

- Enable strict LSA checking on the Helper Router.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper lsa-checking-disable
admin@PICOS# commit
```

set protocols ospf6 graceful-restart helper supported-grace-time

Run the command **set protocols ospf6 graceful-restart helper supported-grace-time** to configure the period for Graceful Restart on the Helper router. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the **default** VRF.

Optional parameter **instance-id** can be included to specify the OSPFv3 multi-instance ID in the default VRF.

> Multiple instances of OSPF are only allowed in the default VRF. A maximum of 8 instance can be configured in the default VRF. In non-default VRFs, only single instance OSPF can be configured.

The command **delete protocols ospf6 graceful-restart helper supported-grace-time** can be used to remove this configuration.

Command Syntax

set protocols ospf6 [instance-id <*instance-id***>] [vrf<***vrf-name***>] graceful-restart helper supported-grace-time <***supported-grace-time***>**

delete protocols ospf6 [instance-id <*instance-id***>] [vrf** <*vrf-name*>**] graceful-restart helper supported-grace-time**

Parameter

Parameter	Description
instance-id <*instance-id*>	Optional, specifies the OSPF instance ID. The value is an integer that ranges from 1 to 8.
vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the OSPF instance.
supported-grace-time <*supported-grace-time***>**	Specifies the period for Graceful Restart on the Helper router. The value is an integer that ranges from 10 through 1800 seconds. There is no default value.

Example

- Configure the period for Graceful Restart on the Helper router.

```
admin@PICOS# set protocols ospf6 instance-id 1 graceful-restart helper supported-grace-time 300
admin@PICOS# commit
```

run graceful-restart prepare ospf6

The **run graceful-restart prepare ospf6** command is a operational command that the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain, informing its neighbors about its restarting process and the estimated time for the restart to complete. These LSAs are Type 9 LSAs and are flooded throughout the OSPF domain.

The OSPF protocol should be restarted during the grace period, otherwise the graceful restart will fail.

To perform a graceful shutdown, this operational command needs to be issued before restarting the OSPF protocol.

- Be cautious: After executing the **run graceful-restart prepare ospf** or **run graceful-restart prepare ospf6** command, the system will be in a waiting state for the OSPF protocol to restart. Users are not allowed to perform any OSPF configuration until the OSPF protocol restart is completed, or unpredictable results can occur.
- Before restarting the OSPF process, the device needs to use the command **run graceful-restart prepare ospf** (for OSPFv2) or **run graceful-restart prepare ospf6** (for OSPFv3) to send Type 9 LSAs for GR capability negotiation. After the negotiation, the OSPF process must be restarted within the negotiated **grace-period**; otherwise, it will timeout and exit the GR state.

Command Syntax

run graceful-restart prepare ospf6

Parameters

None.

Example

- Configure to let the restarting router advertises Graceful Restart (GR) LSAs into the OSPF domain.

```
admin@Xorplus# run graceful-restart prepare ospf6
OSPFv3 Routing Process (0) with Router-ID 2.2.2.2
 Graceful restart helper support disabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
```

run show ospf6 graceful-restart helper

Run the command **run show ospf6 graceful-restart helper** to display the Graceful Restart Helper details including helper config changes.

Command Syntax

run show ospf6 [**instance-id <***instance-id***>**][**vrf<***vrf-name***>**] **graceful-restart helper [detail]**

Parameters

Parameter	Description
instance-id <*instance-id*>	Optional. Specifies the OSPFv3 instance ID. The value is an integer that ranges from 1 to 8.
vrf<*vrf-name***>**	Optional. Specifies the VRF name, the value is a string.

Example

- Display the Graceful Restart Helper details including helper config changes.

```
admin@PICOS# run show ospf6 graceful-restart helper
OSPFv3 Routing Process (0) with Router-ID 12.12.12.20
 Graceful restart helper support disabled.
 Strict LSA check is enabled.
 Helper supported for Planned and Unplanned Restarts.
 Supported Graceful restart interval: 1800(in seconds).
```

Static Route Configuration Commands

- set protocols static interface-route interface
- set protocols static mroute
- set protocols static route

set protocols static interface-route interface

The **set protocols static interface-route interface** command configures a unicast static route by specifying the outgoing interface.

The **delete protocols static interface-route interface** command removes the static route.

Command Syntax

set protocols static [vrf <*vrf-name*>**] interface-route** <*ip/prefixlen*> **interface** <*interface-name*> [**distance** <*distance*> | **tag** <*tag*>]

delete protocols static [vrf <*vrf-name***>] interface-route** <*ip/prefixlen*> **interface** <*interface-name*> [**distance** <*distance*> | **tag** <*tag*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. If not specified, it will create a static route in the default VRF.
interface-route <*ip/prefixlen*>	Specifies a destination IPv4 or IPv6 address. Where *prefixlen* specifies the number of bits in the address mask in int format (x), where x is a decimal number from 1 to 32 for IPv4 and 1 to 128 for IPv6.
interface <*interface-name*>	Specifies the L3 interface as an outgoing interface. The value could be a VLAN interface, loopback interface, routed interface or sub-interface.
distance <*distance*>	Optional. Specifies the administrative distance of a static route. The value is an integer that ranges from 1 to 255.
tag <*tag*>	Optional. Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.

Example

• This example creates a static route.

```
admin@XorPlus# set protocols static interface-route 10.10.10.10/32 interface vlan100
admin@XorPlus# commit
```

set protocols static mroute

The **set protocols static mroute** command adds a static route entry to the Multicast RIB.

The **delete protocols static mroute** command removes the static route.

Command Syntax

set protocols static mroute <*ipv4/prefixlen*> {**next-hop**<*nexthop-address*> **| next-hop-interface** <*interface-name*>} [**distance** <*distance*>]

delete protocols static mroute <*ipv4/prefixlen*> **{next-hop<*nexthop-address*> | next-hop-interface <*interface-name*>} [distance**<*distance*>**]**

Parameter

Parameter	Description
mroute <*ipv4/prefixlen*>	Specifies the IPv4 address of a multicast source. The value is in dotted decimal notation. The value *prefixlen* is a decimal integer that ranges from 1 to 32.
next-hop<*nexthop-address*>	Specifies the next-hop address. The value is in dotted decimal notation.
next-hop-interface <*interface-name*>	Specifies the L3 interface as an outgoing interface. The value could be a VLAN interface, loopback interface, routed interface or sub-interface.
distance <*distance*>	Optional. Specifies the administrative distance of a static route. The value is an integer that ranges from 1 to 255.

Example

• This example creates a static route.

```
admin@XorPlus# set protocols static mroute 10.10.10.0/24 next-hop-interface vlan100
admin@XorPlus# commit
```

set protocols static route

The **set protocols static route** command configures a unicast static route by specifying the next hop.

The **delete protocols static route** command removes the static route.

Note:

- If you are configuring a default route in the default VRF, you need to enable management VRF (After enabled by using command set system management-vrf enable true, eth0 will automatically be moved to management VRF from default VRF) to ensure the normal access to eth0 management port.
- When configuring IPv6 static route on FS S5810 Series and S5860 Series switch, the value of "*prefixlen*" should be less than or equal to 64.

Command Syntax

set protocols static [vrf<*vrf-name*>**] route** <*ip/prefixlen*> {**next-hop** <*nexthop-address*> | **blackhole | null0 | reject}** [**distance** <*distance*> | **tag** <*tag*>]

delete protocols static [vrf<*vrf-name*>**] route** <*ipv4/prefixlen*> {**next-hop** <*nexthop-address*> | **blackhole | null0 | reject}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. If not specified, it will create a static route in the default VRF.
route <*ip/prefixlen*>	Specifies a destination IPv4 or IPv6 address. Where *prefixlen* specifies the number of bits in the address mask in int format (x), where x is a decimal number from 1 to 32 for IPv4 and 1 to 128 for IPv6.
next-hop <*nexthop-address*>	Specifies the next-hop address.
blackhole	Specifies that packets matching the destination route are silently discarded and no ICMP error notification is sent to the sender.
null0	Specifies the NULL0 interface as an outgoing interface. All the IP packets destined for the destination address are discarded without notifying the source host.
reject	Specifies that packets matching the destination route are discarded and an ICMP error notification is sent to the sender.
distance <*distance*>	Optional. Specifies the administrative distance of a static route. The value is an integer that ranges from 1 to 255.
tag <*tag*>	Optional. Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.

Example

• This example creates a static black hole route.

```
admin@XorPlus# set protocols static route 10.10.10.10/32 blackhole
admin@XorPlus# commit
```

Route Map Commands

- run show routing route-map
- set routing as-path-list
- set routing large-community-list expanded
- set routing large-community-list standard
- set routing prefix-list
- set routing prefix-list description
- set routing community-list expanded
- set routing community-list standard
- set routing extcommunity-list expanded
- set routing extcommunity-list standard
- set routing route-map set-action large-community
- set routing route-map call
- set routing route-map description
- set routing route-map match as-path
- set routing route-map match community
- set routing route-map match community-with-exact-match
- set routing route-map match evpn default-route
- set routing route-map match evpn route-type
- set routing route-map match evpn vni
- set routing route-map match extcommunity
- set routing route-map matching-policy
- set routing route-map match interface
- set routing route-map match ipv4-addr address
- set routing route-map match ipv4-addr next-hop
- set routing route-map match ipv4-addr route-source
- set routing route-map match ipv6-addr
- set routing route-map match large-community
- set routing route-map match local-preference
- set routing route-map match metric
- set routing route-map match origin
- set routing route-map match peer
- set routing route-map match source-protocol
- set routing route-map match source-vrf
- set routing route-map match tag
- set routing route-map on-match
- set routing route-map set-action aggregator
- set routing route-map set-action as-path exclude
- set routing route-map set-action as-path prepend
- set routing route-map set-action atomic-aggregate
- set routing route-map set-action comm-list-delete
- set routing route-map set-action community
- set routing route-map set-action community-additive
- set routing route-map set-action extcommunity
- set routing route-map set-action extcommunity bandwidth
- set routing route-map set-action extcommunity bandwidth-non-transitive
- set routing route-map set-action ip-next-hop
- set routing route-map set-action ipv4-vpn-next-hop
- set routing route-map set-action ipv6-next-hop
- set routing route-map set-action label-index
- set routing route-map set-action large-comm-list-delete
- set routing route-map set-action local-preference
- set routing route-map set-action metric
- set routing route-map set-action metric-type
- set routing route-map set-action origin
- set routing route-map set-action originator-id
- set routing route-map set-action src
- set routing route-map set-action tag
- set routing route-map set-action weight

run show routing route-map

The **run show routing route-map** command to displays the configured route map information.

Command Syntax

run show routing route-map

Parameter

None.

Example

- View the configured route map information.

```
admin@Xorplus# run show routing route-map
ZEBRA:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
OSPF:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
  Set clauses:
  Call clause:
  Action:
    Exit routemap
BGP:
route-map: GlobalMap Invoked: 0 Optimization: disabled Processed Change: false
 permit, sequence 10 Invoked 0
  Match clauses:
    community COMMUNITY1
  Set clauses:
    community 11:101
  Call clause:
  Action:
    Exit routemap
```

set routing as-path-list

The **set routing as-path-list** command configures an AS Path list to match a specific AS path. AS Path lists are named lists of regular expression rules. They are used to match AS Path attributes in the routes for inclusion in or exclusion from route policies.

The **delete routing as-path-list** command removes the AS Path list configuration.

Command Syntax

set routing as-path-list <*as-path-list-name*> **{deny|permit} regex** <*txt*>

delete routing as-path-list <*as-path-list-name*> [**{deny|permit} regex** <*txt*>]

Parameter

Parameter	Description
as-path-list <*as-path-list-name*>	Specifies the name of the AS Path list.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
regex <*txt*>	Specifies the AS_Path regular expression (BGP Regular Expressions). The value is a string of 1 to 255 characters, space is not supported. **NOTE**: AS_Path regular expression doesn't support the specifial character ".", which results in unsupported filtering of AS numbers in asdot format.

Example

- Configure an AS Path list, permit routes that contain 20 in the AS_Path to pass through.

```
admin@Xorplus# set routing as-path-list Aslist permit regex _20_
admin@Xorplus# commit
```

set routing large-community-list expanded

The **set routing large-community-list expanded** command defines a new expanded large community list.

The **delete routing large-community-list expanded** command removes the expanded large community list configuration.

Command Syntax

set routing large-community-list {expanded <*large-community-list-name*>| **seq-expanded** <*integer*>} **{deny|permit} regex** <*line*>

delete routing large-community-list {expanded <*large-community-list-name*>**| seq-expanded** <*integer*>**} {deny|permit} regex** <*line*>

Parameter

Parameter	Description
expanded <*large-community-list-name*>	Specifies the name of the large community list that matches a route.
seq-expanded <*integer*>	Specifies an expanded large community list number from 100 to 500.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
<*line*>	Specifies a string matching expression, it will be compared to the entire Large Communities attribute as a string, with each large-community in order from lowest to highest. line can also be a regular expression (BGP Regular Expressions) which matches this Large Community attribute.

Example

- Define a new expanded large community list.

```
admin@Xorplus# set routing large-community-list expanded Largecom1 permit regex *20
admin@Xorplus# commit
```

set routing large-community-list standard

The **set routing large-community-list standard** command defines a new standard large community list.

The **delete routing large-community-list standard** command removes the standard large community list configuration.

Command Syntax

set routing large-community-list {standard <*large-community-list-name***>| seq-standard**<*integer*>} **{deny|permit}** [**large-community** <*large-community-number*>]

delete routing large-community-list {standard <*large-community-list-name*>**| seq-standard**<*integer*>**} {deny|permit} [large-community** <*large-community-number*>**]**

Parameter

Parameter	Description
standard <*large-community-list-name***>**	Specifies the name of the large community list that matches a route.
seq-standard<*integer*>	Specifies an standard large community list number from 1 to 99.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
large-community <*large-community-number*>	Specifies the large community value. The value should be in a aa:bb:cc format. A maximum of 99 large community value can be configured.

Usage Guidelines

This command defines a new standard large-community-list. large-community is the Large Community value. We can add multiple large communities under same name. In that case the match will happen in the user defined order. Once the large-community-list matches the Large Communities attribute in BGP updates it will return permit or deny based upon the large-community-list definition. When there is no matched entry, a deny will be returned. When large-community is empty it matches any routes.

Example

- Define a new standard large community list.

```
admin@Xorplus# set routing large-community-list standard LargeCom deny large-community 6215:22:33
admin@Xorplus# commit
```

set routing prefix-list

The **set routing prefix-list** command creates an IPv4/IPv6 prefix list or an entry in an IPv4/IPv6 prefix list.

The **delete routing prefix-list** command deletes an IPv4/IPv6 prefix list or an entry from an IPv4/IPv6 prefix list.

Command Syntax

set routing prefix-list {ipv4-family <*ipv4-prefix-name*> | **ipv6-family** <*ipv6-prefix-name*>} [**seq** <*sequence-number*>] {**deny|permit} {prefix** <*ipaddress/prefixlen*> **[ge <***greater-equal-value***>] [le <***less-equal-value***>]** | **prefix-any**}

delete routing prefix-list {**ipv4-family** <*ipv4-prefix-name*> **| ipv6-family** <*ipv6-prefix-name*>} [**seq** <*sequence-number*>]**deny|permit} {prefix** <*ipaddress/prefixlen*> **[ge** <*greater-equal-value*>**] [le** <*less-equal-value*>**] | prefix-any}**

Parameter

Parameter	Description
<*ip4-prefix-name*>	Specifies the name of an IPv4 prefix list.
<*ip6-prefix-name*>	Specifies the name of an IPv6 prefix list.
seq <*sequence-number*>	Optional. Specifies the sequence number of an entry in the IP prefix list. The value is an integer that ranges from 1 to 4294967295. **NOTE:** When configuring IP prefix list, it is strongly recommended to configure sequence number for each IP prefix list node. Otherwise, the precedence of this IP prefix list will be uncertain, and thus the desired IP filtering effect will not be achieved.
{**deny|permit}**	Specifies whether the route is available for further processing when there is a match. The value could be **deny** or **permit**. • **deny**: In deny mode, if the IP address to be filtered is within the defined prefix range, the IP address fails to match the routing policy and cannot match the next entry. • **permit**: In permit mode, if the IP address to be filtered is within the defined prefix range, the IP address matches the routing policy and does not continue to match the next entry.
{prefix <*ipaddress/prefixlen*> | **prefix-any}**	Specifies an IP address/prefix length or all addresses. The value of prefix length is an integer that ranges from 1 to 32 for IPv4 addresses, and 1 to 128 for IPv6 addresses. When **prefix-any** is specified, it creates a prefix-list that matches all addresses.
ge <*greater-equal-value***>**	Optional. Specifies the lower threshold of the mask length. It can be used when an IP address/prefix length is specified. If **ge** *greater-equal-value* and **le** *less-equal-value* are not specified, the value of prefix length is the mask length. For IPv4: • *greater-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. • If only **ge** is configured, the mask ranges from *greater-equal-value* to 32. For IPv6:

Parameter	Description
	• *greater-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128. • If only **ge** is configured, the mask ranges from *greater-equal-value* to 128.
le <*less-equal-value***>**	Optional. Specifies the upper threshold of the mask length. It can be used when an IP *address/prefix* length is specified. If **ge** *greater-equal-value* and **le** *less-equal-value* are not specified, the value of prefix length is the mask length. For IPv4: • *less-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. • If only **le** is configured, the mask ranges from *prefixlen* to *less-equal-value*. For IPv6: • *less-equal-value* must meet the following requirement: *prefixlen* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128. • If only **le** is configured, the mask ranges from *prefixlen* to *less-equal-value*.

Example

- Configure the IPv4 prefix list named **p1** to permit only the routes with the mask length ranging from 8 to 16 on the network segment 35.0.0.0/8.

```
admin@Xorplus# set routing prefix-list ipv4-family p1 seq 1 permit prefix 35.0.0.0/8 ge 16
admin@Xorplus# commit
```

- Configure the IPv6 prefix list named **p2** to permit the routes with the mask length ranging from 32 to 64 bits.

```
admin@Xorplus# set routing prefix-list ipv6-family p2 seq 1 permit prefix ::/0 ge 32 le 64
admin@Xorplus# commit
```

set routing prefix-list description

The **set routing prefix-list description** command creates a description of an IPv4/IPv6 prefix list.

The **delete routing prefix-list description** command deletes the description of an IPv4/IPv6 prefix list.

Command Syntax

set routing prefix-list {ipv4-family <*ipv4-prefix-name*> **| ipv6-family** <*ipv6-prefix-name*>**} description <***string***>**

delete routing prefix-list {ipv4-family <*ipv4-prefix-name*> **| ipv6-family** <*ipv6-prefix-name*>**} description**

Parameter

Parameter	Description
<*ip4-prefix-name*>	Specifies the name of an IPv4 prefix list.
<*ip6-prefix-name*>	Specifies the name of an IPv6 prefix list.
description <*string***>**	Optional. Specifies the description of an IPv4 prefix list. The value is a string.

Example

- Configure the description of the IP prefix list **p1**.

```
admin@Xorplus# set routing prefix-list ipv4-family p1 description Net1Pref
admin@Xorplus# commit
```

set routing community-list expanded

The **set routing community-list expanded** command defines a new expanded community list. The expanded community is only used to filter.

The **delete routing community-list expanded** command removes the expanded community list configuration.

Command Syntax

set routing community-list expanded *<community-list-name>* **{deny|permit} regex** *<regular-expression>*

delete routing community-list expanded *<community-list-name>* **{deny|permit} regex** *<regular-expression>*

Parameter

Parameter	Description
<community-list-name>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
<regular-expression>	Specifies a string expression of communities attribute. It can be a regular expression (BGP Regular Expressions) to match the communities attribute in BGP updates. Space is not supported.

Example

- Configure a new expanded community list.

```
admin@Xorplus# set routing community-list expanded Comm1 permit regex 100:100
admin@Xorplus# commit
```

set routing community-list standard

The **set routing community-list standard** command configures a standard community list to match a specific community number attribute. Community-list is a named list of regular expressions. They are used to match the community number attributes in the routes for inclusion in, or exclusion from route policies.

The **delete routing community-list standard** command removes the standard community list configuration.

Command Syntax

set routing community-list standard <*community-list-name*> **{deny|permit} [local-as|no-advertise|no-export|internet|community** <*community*>**]**

delete routing community-list standard <*community-list-name*>**{deny|permit} [local-as|no-advertise|no-export|internet|community** <*community*>**]**

Parameter

Parameter	Description
<*community-list-name*>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
{local-as|no-advertise|no-export|internet|community <*community-numer*>**}**	Optional. Specifies BGP community type, it can be one of following BGP communities: • **local-AS:** a BGP community that restricts routes to your confederation's sub-AS. • **no-advertise:** a BGP community that is not advertised to anyone. • **no-export:** a BGP community that is not advertised to the eBGP peer. • **internet:** a BGP community that matches all routes. • **community** <*community-numer*>: Specifies the community number. The value is in AA:NN format where AA and NN are ranging from 0 to 65535.

Usage Guidelines

The BGP community list can be either standard or expanded. The standard BGP community list is a pair of values (such as 100:100) that can be tagged on a specific prefix and advertised to other neighbors or applied on route ingress.

Example

- Here is an example of a standard community list filter:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# commit
```

set routing extcommunity-list expanded

The **set routing extcommunity-list expanded** command defines a new expanded extcommunity-list.

The **delete routing extcommunity-list expanded** command removes the expanded community list configuration.

Command Syntax

set routing extcommunity-list expanded <*community-list-name*> **{deny|permit} regex** <*regular-expression*>

delete routing extcommunity-list expanded<*community-list-name*> **{deny|permit} regex** <*regular-expression*>

Parameter

Parameter	Description
<*community-list-name*>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
<*regular-expression*>	Specifies a string expression of communities attribute. It can be a regular expression (BGP Regular Expressions) to match the communities attribute in BGP updates. The expanded community is only used to filter.

Example

- Define a new expanded extcommunity-list.

```
admin@Xorplus# set routing extcommunity-list expanded EXTcom1 permit regex 200:200
admin@Xorplus# commit
```

set routing extcommunity-list standard

The **set routing extcommunity-list standard** command defines a new standard extcommunity-list.

The **delete routing extcommunity-list standard** command removes the standard community list configuration.

Command Syntax

set routing extcommunity-list standard <*community-list-name*> **{deny|permit} {rt|soo} extcommunity** <*extcommunity*>

delete routing extcommunity-list standard <*community-list-name*> **{deny|permit} {rt|soo} extcommunity** <*extcommunity*>

Parameter

Parameter	Description
<*community-list-name*>	Specifies the name of the community list that matches a route.
{deny|permit}	Specifies whether the route is available for further processing when there is a match.
{rt|soo}	**rt**: Indicates the Route Target value. **soo**: Indicates the Site of Origin.
<*extcommunity*>	Specifies an extended community value.

Usage Guidelines

We can define multiple extcommunity-list under same name. In that case match will happen user defined order. Once the extcommunity-list matches to extended communities attribute in BGP updates it return permit or deny based upon the extcommunity-list definition. When there is no matched entry, deny will be returned. When *extcommunity* is empty it matches to any routes.

Example

- Define a new standard extcommunity-list.

```
admin@Xorplus# set routing extcommunity-list standard EXTcom1 permit rt extcommunity 20
admin@Xorplus# commit
```

set routing route-map set-action large-community

The **set routing route-map set-action large-community** command modifies the large community number to the existing community number attribute of the route.

The **delete routing route-map set-action large-community** command restores the default behavior of not modifying the large community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name*> order <*NUMBER*> set-action large-community none

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community1 {**<*large-community*>| **additive**}

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community2 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community3 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community4 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community5 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community6 {**<*large-community*>| **additive}**

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-community large-community7 {**<*large-community*>| **additive}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community none**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community1**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community2**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community3**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community4**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community5**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community6**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-community large-community7**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
none	Indicates that all the community attributes of routes are deleted.
<*large-community*>	Specifies the community number.
additive	Indicates that existing community attributes can be added to routes. Note that: If the keyword **additive** is not set, the original extended community attribute is replaced.

Example

- Modify the large community number to the existing community number attribute of the route to 10:22:30.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action large-community large-community1 10:22:30
admin@Xorplus# commit
```

set routing route-map call

The **set routing route-map call** command calls to another route-map, after any Set Actions have been carried out. If the route-map called returns *deny* then processing of the route-map finishes and the route is denied, regardless of the Matching Policy or the Exit Policy. If the called route-map returns *permit*, then Matching Policy and Exit Policy govern further behaviour, as normal.
The **delete routing route-map call** command removes the route map entry configuration.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> call** <*route-map-statement*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **call** <*route-map-statement*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
call <*route-map-statement*>	Specifies the name of the route map. Required.

Example

- Configure a route map entry that calls to another route-map.

```
admin@Xorplus# set routing route-map GlobalMap order 10 call LocalMap
admin@Xorplus# commit
```

set routing route-map description

The **set routing route-map description** command adds descriptions to a route-map entry.
The **delete routing route-map description** command removes descriptions to a route-map entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> description** <*string*>

delete routing route-map <*route-map-name*> ***order*** <*NUMBER*> **description** <*string*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
description <*string*>	Specifies descriptions to a route map. The value is a string.

Example

- Add descriptions to a route-map entry.

```
admin@Xorplus# set routing route-map GlobalMap order 10 description GlobalMap
admin@Xorplus# commit
```

set routing route-map match as-path

The **set routing route-map match as-path** command matches the AS path attribute of the route with one or more regular expressions in the AS path list.
The **delete routing route-map match as-path** command restores the default behavior of not matching the AS path attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match as-path** <*as-path-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match as-path** <*as-path-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
match as-path <*as-path-list*>	Specifies the name of the AS path list to match the AS path attribute of the route.

Example

- Configure a match clause in the route map to match the AS path list:

```
admin@Xorplus# set routing as-path-list Aslist permit regex _20_
admin@Xorplus# set routing route-map GlobalMap order 10 match as-path Aslist
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match community

The **set routing route-map match community** command matches the community number attribute of the route with one, or more regular expressions in the community-list.
The **delete routing route-map match community** command restores the default behavior of not matching the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match community** <*community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match community** <*community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community <*community-list*>	Specifies the name of the community-list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the community list:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# set routing route-map GlobalMap order 10 match community COMMUNITY1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match community-with-exact-match

The **set routing route-map match community-with-exact-match** command matches the community number attribute must match exactly with the expressions in the community-list. However, the order of the communities in the community-list is of no significance.
The **delete routing route-map match community-with-exact-match** command restores the default behavior of not matching the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match community-with-exact-match** <*community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match community-with-exact-match** <*community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community-with-exact-match <*community-list*>	Specifies the name of the community-list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the community list:

```
admin@Xorplus# set routing community-list standard COMMUNITY1 permit community 100:100
admin@Xorplus# set routing route-map GlobalMap order 10 match community-with-exact-match COMMUNITY1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match evpn default-route

The **set routing route-map match evpn default-route** command matches the EVPN default route with the one configured in the match clause.
The **delete routing route-map match evpn default-route** command restores the default behavior of not matching the EVPN default route of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match evpn default-route**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match evpn default-route**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.

Example

- Configure a match clause in the route map to match the EVPN default route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match evpn default-route
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match evpn route-type

The **set routing route-map match evpn route-type** command matches the EVPN route-type with the one configured in the match clause.
The **delete routing route-map match evpn route-type** command restores the default behavior of not matching the EVPN route-type of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match evpn route-type <macip|prefix|multicast>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match evpn route-type <macip|prefix|multicast>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
route-type <macip|prefix|multicast>	Specifies the EVPN route type.

Example

- Configure a match clause in the route map to match the EVPN route-type:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match evpn route-type macip
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match evpn vni

The **set routing route-map match evpn vni** command matches the EVPN VNI ID with the one configured in the match clause.
The **delete routing route-map match evpn vni** command restores the default behavior of not matching the EVPN VNI ID of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match evpn vni <***vni-id***>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match evpn vni** <*vni-id*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
vni <*vni-id*>	Specifies the EVPN VNI ID. The value is an integer that ranges from 1 to 16777215.

Example

- Configure a match clause in the route map to match the EVPN VNI ID:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match evpn vni 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match extcommunity

The **set routing route-map match extcommunity** command matches the extended community number attribute of the route with one, or more regular expressions in the community-list.
The **delete routing route-map match extcommunity** command restores the default behavior of not matching the extended community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match extcommunity** <*extcommunity-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match extcommunity** <*extcommunity-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
extcommunity <*extcommunity-list*>	Specifies the name of the extended community-list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the extended community list:

```
admin@Xorplus# set routing extcommunity-list standard EXTcom1 permit 20
admin@Xorplus# set routing route-map GlobalMap order 10 match extcommunity EXTcom1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map matching-policy

The **set routing route-map matching-policy** command configures a route map entry with the given name and action by taking the CLI in the route map context. All route map entries with the same name belong to the same route map. The route map entry rules are processed in order by sequence number, until a match is found.
The **delete routing route-map matching-policy** command removes the route map entry configuration.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> matching-policy <deny|permit>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **matching-policy <deny|permit>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
matching-policy <deny|permit>	Specifies whether the route is available for further processing when there is a match. Required.

Example

- Configure a route map matching-policy.

```
admin@Xorplus# set routing route-map GlobalMap order 1 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match interface

The **set routing route-map match interface** command matches the outgoing VLAN interface value of the route with the value configured in the match clause.
The **delete routing route-map match interface** command restores the default behavior of not matching the outgoing VLAN interface value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match interface** <*interface*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match interface** <*interface*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
interface <*interface*>	Specifies the value to be matched with the outgoing VLAN interface of the route entry.

Example

- Configure a match clause in the route map to match the outgoing interface of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match interface vlan100
admin@Xorplus# commit
```

set routing route-map match ipv4-addr address

The **set routing route-map match ipv4-addr address** command matches the destination IP address prefix length or the prefix list of the routes.
The **delete routing route-map match ipv4-addr address** command restores the default behavior of not matching the destination IP address prefix length or the prefix list of the routes.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv4-addr address {prefix-len** <*prefix-len*>|**prefix-list** <*prefix-list-v4*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv4-addr address {prefix-len** <*prefix-len*>**|prefix-list** <*prefix-list-v4*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-len <*prefix-len*>	Specifies the prefix length to be matched. The value is an integer that ranges from 0 to 32.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.

Example

- Configure a match clause in the route map to match the address prefix length of the routes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv4-addr address prefix-len 24
admin@Xorplus# commit
```

set routing route-map match ipv4-addr next-hop

The **set routing route-map match ipv4-addrnext-hop** command matches the next-hop address prefix length or prefix list of the routes.
The **delete routing route-map match ipv4-addr next-hop** command restores the default behavior of not matching the next-hop address prefix length or prefix list of the routes.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv4-addr next-hop {prefix-len** <*prefix-len*>|**prefix-list** <*prefix-list-v4*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv4-addr next-hop {prefix-len** <*prefix-len*>**|prefix-list** <*prefix-list-v4*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-len <*prefix-len*>	Specifies the prefix length to be matched. The value is an integer that ranges from 0 to 32.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.

Example

- Configure a match clause in the route map to match the next hop prefix length of the routes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv4-addr next-hop prefix-len 24
admin@Xorplus# commit
```

set routing route-map match ipv4-addr route-source

The **set routing route-map match ipv4-addr route-source** command matches the source IP address prefix of the routes with one or more addresses in the prefix list.
The **delete routing route-map match ipv4-addr route-source** command restores the default behavior of not matching the source IP address prefix of the routes to their default value.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv4-addr route-source prefix-list** <*prefix-list-v4*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv4-addr route-source prefix-list** <*prefix-list-v4*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
<*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.

Example

- Configure a match clause in the route map to match the source IP address prefix list P1.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv4-addr route-source prefix-list P1
admin@Xorplus# commit
```

set routing route-map match ipv6-addr

The **set routing route-map match ipv6-addr** command matches the destination IPv6 address or the next hop of the routes.
The **delete routing route-map match ipv6-addr** command restores the default behavior of not matching the destination IPv6 address or the next hop of the routes.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match ipv6-addr {address prefix-list** <*prefix-list*> | **next-hop** <*next-hop-address*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match ipv6-addr {address prefix-list** <*prefix-list*> | **next-hop** <*next-hop-address*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prefix-list <*prefix-list-v4*>	Specifies the name of the prefix list to be matched.
next-hop <*next-hop-address*>	Specifies the next hop address of the routes to be matched.

Example

- Configure a match clause in the route map to match the address prefix length of the routes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 match ipv6-addr address next-hop ::ac12
admin@Xorplus# commit
```

set routing route-map match large-community

The **set routing route-map match large-community** command matches the BGP Large Community number attribute of the route with one, or more regular expressions in the community-list.
The **delete routing route-map match large-community** command restores the default behavior of not matching the BGP Large Community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match large-community** *<large-community-list>*

delete routing route-map *<route-map-name>* **order** *<NUMBER>* **match large-community** *<large-community-list>*

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
large-community *<large-community-list>*	Specifies the name of the BGP Large Community list to match the community number attribute of the route.

Example

- Configure a match clause in the route map to match the BGP Large Community list:

```
admin@Xorplus# set routing large-community-list standard Largecom1 permit large-community 6215:22:33
admin@Xorplus# set routing route-map GlobalMap order 10 match large-community Largecom1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match local-preference

The **set routing route-map match local-preference** command matches the local preference value of the route with the value configured in the match clause.
The **delete routing route-map match local-preference** command restores the default behavior of not matching the local preference value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match local-preference** <*value*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match local-preference** <*value*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
local-preference <*value*>	Specifies the value to be matched with the route entry local preference in the range of 1 to 4294967295.

Example

- Configure a match clause in the route map to match the local preference of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match local-preference 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-action permit
admin@Xorplus# commit
```

set routing route-map match metric

The **set routing route-map match metric** command matches the MED value of the route with the value configured in the match clause.
The **delete routing route-map match metric** command restores the default behavior of not matching the MED value of the route.

Command Syntax

set routing route-map <*route-map-name***> order** <*NUMBER*> **match metric** <*value*>

delete routing route-map <*route-map-name*> **order <***NUMBER***> match metric** <*value*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
metric <*value*>	Specifies the value to be matched with the route entry MED in the range of 1 to 4294967295.

Example

- Configure a match clause in the route map to match the metric of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match metric 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match origin

The **set routing route-map match origin** command matches the route origin attribute of the route with route configured in the match clause.
The **delete routing route-map match origin** command restores the default behavior of not matching the route origin attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match origin <egp|igp|incomplete>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match origin <egp|igp|incomplete>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
origin <egp|igp|incomplete>	Specifies if the route origin attribute is matched with a match clause which originated as IGP, EGP, or has unknown origin. The unknown origin is typically redistributed from another routing protocol.

Example

- Configure a match clause in the route map to match the origin:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match origin egp
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match peer

The **set routing route-map match peer** command matches the peer ip address. This is a BGP specific match command.
The **delete routing route-map match peer** command restores the default behavior of not matching the peer ip address if the BGP neighbor of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match peer {ipv4-addr** <*ipv4-address*>**|ipv6-addr** <*ipv6-address*> | **local}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match peer {ipv4-addr** <*ipv4-address*>**|ipv6-addr** <*ipv6-address*> | **local}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
peer {ipv4-addr <*ipv4-address*>**|ipv6-addr** <*ipv6-address*>**|local}**	Specifies if the peer ip address if the BGP neighbor is matched with a match clause.

Example

- Configure a match clause in the route map to match the peer ip address if the BGP neighbor:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match peer ipv4-addr 100.100.100.1
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match source-protocol

The **set routing route-map match source-protocol** command matches the source routing protocol value of the route with the value configured in the match clause. The **delete routing route-map match source-protocol** command restores the default behavior of not matching the source routing protocol value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match source-protocol <bgp|connected|kernel|ospf|ospf6|static|system>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match source-protocol <bgp|connected|kernel|ospf|ospf6|static|system>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
source-protocol <bgp|connected|kernel|ospf|ospf6|static|system>	Specifies the bgp, connected, ospf, kernel, system or static value to be matched with the route entry source protocol.

Example

- Configure a match clause in the route map to match the source routing protocol value:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match source-protocol bgp
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match source-vrf

The **set routing route-map match source-vrf** command matches the source VRF attribute of the route with route configured in the match clause.
The **delete routing route-map match source-vrf** command restores the default behavior of not matching the source VRF attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match source-vrf** <*source-vrf*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match source-vrf** <*source-vrf*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
source-vrf <*source-vrf*>	Specifies if the source VRF attribute is matched with a match clause.

Example

- Configure a match clause in the route map to match the source VRF:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match source-vrf VRF-east
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map match tag

The **set routing route-map match tag** command matches the tag value of the route with the one configured in the match clause. Applies to static routes that will be redistributed to ospfv2 and ospfv3 protocols.
The **delete routing route-map match tag** command restores the default behavior of not matching the tag value of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> match tag** <*value*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **match tag** <*value*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
tag <*value*>	Numeric value to match with the route tag that ranges from 0 to 65535. Required.

Example

- Configure a match clause in the route map to match the tag value:

```
admin@Xorplus# set routing route-map GlobalMap order 10 match tag 100
admin@Xorplus# set routing route-map GlobalMap order 10 matching-policy permit
admin@Xorplus# commit
```

set routing route-map on-match

The **set routing route-map on-match** command specifies an alternative Exit Policy to take if the entry matched, rather than the normal policy of exiting the route-map and permitting the route.
The **delete routing route-map on-match** command removes the route map entry configuration.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> on-match {goto <***NUMBER2***>| next}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **on-match {goto <***NUMBER2***>| next}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
{goto <*NUMBER2***>| next}**	The two possibilities are: • **next**: Continue on with processing of the route-map entries. • **goto <***NUMBER2***>**: Jump ahead to the first route-map entry whose order in the route-map is >=NUMBER2. Jumping to a previous entry is not permitted. The value is an integer that ranges from 1 to 65535.

Example

- Configure a on-match clause in the route map:

```
admin@Xorplus# set routing route-map GlobalMap order 10 on-match next
admin@Xorplus# commit
```

set routing route-map set-action aggregator

The **set routing route-map set-action aggregator** command is a complement to the ATOMIC_AGGREGATE attribute where routing information is missing - it contains the AS number that initiated the route aggregation and the IP address of the BGP publisher that formed the aggregated route.

The **delete routing route-map set-action aggregator** command removes the configurations.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action aggregator {as** <*as-number*>|**ip** <*ipv4-address*>}

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action aggregator {as** <*as-number*>|**ip** <*ipv4-address*>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
as <*as-number*>	Specifies the AS number that initiated the route aggregation. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.
ip <*ipv4-address*>	Specifies the IPv4 address of the BGP publisher that formed the aggregated route.

Usage Guidelines

ATOMIC_AGGREGATE is a warning that routing information is missing, and the AGGREGATOR attribute complements where routing information is missing - it contains the AS number that initiated the route aggregation and the IP address of the BGP publisher that formed the aggregated route. When performing route aggregation, the AGGREGATOR attribute is added at the same time as the ATOMIC-AGGREGATE attribute for the aggregated route information.

Example

- Configure the ATOMIC_AGGREGATE attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action aggregator as 100
admin@Xorplus# commit
```

set routing route-map set-action as-path exclude

The **set routing route-map set-action as-path exclude** command removes all occurrences of the configured AS Path from the AS Path attribute of the route.
The **delete routing route-map set-action as-path exclude** command restores the default behavior of not modifying the AS Path attribute list.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action as-path exclude** <*AS*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action as-path exclude** <*AS*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
as-path exclude <*AS*>	Specifies the AS number to be removed from the AS Path attribute of the route. It is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example

- Configure a action clause in the route map to remove the AS from the AS Path attribute of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action as-path exclude 10
admin@Xorplus# commit
```

set routing route-map set-action as-path prepend

The **set routing route-map set-action as-path prepend** command prepends the list of the configured AS numbers to the AS Path attribute of the routes. To ensure that the AS path conforms to standards, the local AS is prepended after this command is executed.
The **delete routing route-map set-action as-path prepend** command restores the default behavior of not modifying the AS Path attribute list.

NOTE: The **delete** form of the command deletes the entire list of AS-Path prepend configuration regardless of the parameter list.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action as-path prepend [as1** <*AS*> | **as2** <*AS*>| **as3** <*AS*>| **as4** <*AS*>| **as5** <*AS*>| **last-as** <*last-as*>]

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action as-path prepend [as1**<*AS*> | **as2**<*AS*>| **as3** <*AS*>| **as4** <*AS*>| **as5** <*AS*>| **last-as** <*last-as*>]

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
prepend [as1<*AS*> | **as2**<*AS*>| **as3** <*AS*>| **as4** <*AS*>| **as5** <*AS*>| **last-as** <*last-as*>]	Specifies the AS numbers to be prepended from the AS Path attribute of the route. At most six AS number can be set. The value of <*AS*> is a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Example

- Configure a action clause in the route map to prepend the AS from the AS Path attribute of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action as-path prepend as1 102
admin@Xorplus# commit
```

set routing route-map set-action atomic-aggregate

The **set routing route-map set-action atomic-aggregate** command is used to inform the route recipient that the route is aggregated and is a recognized optional attribute.

The **delete routing route-map set-action atomic-aggregate** command removes the configurations.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action atomic-aggregate**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action atomic-aggregate**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.

Usage Guidelines

Sometimes a BGP publisher will receive two overlapping routes, one of which contains addresses that are a subset of the other route. Normally the BGP publisher prefers the finer route (the former), but when publishing externally, if it chooses to publish the coarser one (the latter), it then needs to append the ATOMIC-AGGREGATE attribute to inform the peer. It is actually a warning, because publishing the coarser route means that the finer routing information is lost in the publishing process. When performing route aggregation, the ATOMIC-AGGREGATE attribute is added to the aggregated route information.

Example

- Configure a action clause to inform the route recipient that the route is aggregated and is a recognized optional attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action atomic-aggregate
admin@Xorplus# commit
```

set routing route-map set-action comm-list-delete

The **set routing route-map set-action comm-list-delete** command removes communities value from BGP communities attribute.

When BGP route's communities value matches to the community list name, the communities value is removed. When all of communities value is removed eventually, the BGP update's communities attribute is completely removed.

The **delete routing route-map set-action comm-list-delete** command restores the default behavior of not deleting the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action comm-list-delete** <*community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action comm-list-delete** <*community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
comm-list-delete<*community-list*>	Specifies the name of the community-list.

Example

- Configure to remove communities value from BGP communities attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action comm-list-delete Comlst
admin@Xorplus# commit
```

set routing route-map set-action community

The **set routing route-map set-action community** command changes the community number to the existing community number attribute of the route.

The **delete routing route-map set-action community** command restores the default behavior of not changing the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action community** <*community*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action community** <*community*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community <*community*>	Specifies the community number.

Example

- Add the community number to the existing community number attribute of the route.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action community 11:101
admin@Xorplus# commit
```

set routing route-map set-action community-additive

The **set routing route-map set-action community-additive** command adds the community number to the existing community number attribute of the route.

The **delete routing route-map set-action community-additive** command restores the default behavior of not adding the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action community-additive** <*community*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action community-additive** <*community*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
community-additive <*community*>	Specifies the community number.

Example

- Add the community number to the existing community number attribute of the route.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action community-additive 11:101
admin@Xorplus# commit
```

set routing route-map set-action extcommunity

The **set routing route-map set-action extcommunity** command modifies the extended community number to the existing community number attribute of the route.

The **delete routing route-map set-action extcommunity** command restores the default behavior of not modifying the community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity1** <*extcommunity*>

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity2** <*extcommunity*>

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity3** <*extcommunity*>

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity4** <*extcommunity*>

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity5** <*extcommunity*>

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity6** <*extcommunity*>

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity <rt|soo> extcommunity7** <*extcommunity*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> ***set-action*** **extcommunity <rt|soo> extcommunity1**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> ***set-action*** **extcommunity <rt|soo> extcommunity2**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> ***set-action*** **extcommunity <rt|soo> extcommunity3**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> ***set-action*** **extcommunity <rt|soo> extcommunity4**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> ***set-action*** **extcommunity <rt|soo> extcommunity5**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> ***set-action*** **extcommunity <rt|soo> extcommunity6**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> ***set-action*** **extcommunity <rt|soo> extcommunity7**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
rt	Indicates the route-target extended community.
soo	Indicates the Site of Origin value.
<*extcommunity*>	Specifies the community number.

Example

- Modify the extended community number to the existing community number attribute of the route.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action extcommunity rt extcommunity1 100:2
admin@Xorplus# commit
```

set routing route-map set-action extcommunity bandwidth

The **set routing route-map set-action extcommunity bandwidth** command sets the BGP link-bandwidth extended community for the prefix (best path) for which it is applied.

The **delete routing route-map set-action extcommunity bandwidth** command restores the default behavior of not modifying the BGP link-bandwidth extended community of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity bandwidth {<***bandwidth***>|cumulative|num-multipaths}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action extcommunity bandwidth {**<*bandwidth*>**|cumulative|num-multipaths}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
<*bandwidth***>|cumulative|num-multipaths**	The link-bandwidth can be specified as an explicit value (specified in Mbps), or the router can be told to use the cumulative bandwidth of all multipaths for the prefix or to compute it based on the number of multipaths.

Example

- The following command examples show how you can set the BGP link bandwidth extended community against all prefixes.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action extcommunity bandwidth num-multipaths
admin@Xorplus# commit
```

set routing route-map set-action extcommunity bandwidth-non-transitive

The **set routing route-map set-action extcommunity bandwidth-non-transitive** command sets link bandwidth extended community as non-transitive. The link bandwidth extended community is encoded as transitive unless the set command explicitly configures it as non-transitive.

The **delete routing route-map set-action extcommunity bandwidth-non-transitive** command restores the default behavior of not modifying the BGP link-bandwidth extended community of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action extcommunity bandwidth-non-transitive** <*bandwidth*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action extcommunity bandwidth-non-transitive** <*bandwidth*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
<*bandwidth***>**	The link-bandwidth can be specified as an explicit value (specified in Mbps).

Example

- The following command examples sets link bandwidth extended community as non-transitive.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action extcommunity bandwidth-non-transitive 128
admin@Xorplus# commit
```

set routing route-map set-action ip-next-hop

The **set routing route-map set-action ip-next-hop** command sets the IP address of the next-hop address or peer address of the route with the value configured in the action clause or keep unchanged.
The **delete routing route-map set-action ip-next-hop** command restores the default behavior of not modifying the IP address of the next-hop of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action ip-next-hop {ipv4-addr** *<next-hop-address>* | **peer-address | unchanged}**

delete routing route-map *<route-map-name>* **order** *<NUMBER>* **set-action ip-next-hop {ipv4-addr** *<next-hop-address>* | **peer-address | unchanged}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
ip-next-hop {ipv4-addr *<next-hop-address>*	**peer-address	unchanged}**	Specifies the IPv4 address to be set as the next-hop address or peer address of the route or keep unchanged.

Example

- Set the IP address of the next-hop of the route with the value configured in the action clause.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action ip-next-hop ipv4-addr 10.10.10.1
admin@Xorplus# commit
```

set routing route-map set-action ipv4-vpn-next-hop

The **set routing route-map set-action ipv4-vpn-next-hop** command sets the IP address of the VPN next-hop of the route with the value configured in the action clause.
The **delete routing route-map set-action ipv4-vpn-next-hop** command restores the default behavior of not modifying the IP address of the VPN next-hop of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action ipv4-vpn-next-hop** <*next-hop-address*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action ipv4-vpn-next-hop** <*next-hop-address*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
ipv4-vpn-next-hop <*next-hop-address*>	Specifies the IPv4 address to be set as the VPN next-hop address of the route.

Example

- Set the IP address of the VPN next-hop of the route with the value configured in the action clause.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action ipv4-vpn-next-hop 10.10.10.1
admin@Xorplus# commit
```

set routing route-map set-action ipv6-next-hop

The **set routing route-map set-action ipv6-next-hop** command sets the IP address of the next-hop address or peer address of the route with the value configured in the action clause or keep unchanged.
The **delete routing route-map set-action ipv6-next-hop** command restores the default behavior of not modifying the IP address of the next-hop of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action ipv6-next-hop {[global ipv6-addr** <*next-hop-address*>] | [**local ipv6-addr** <*next-hop-address*>] | **peer-address | prefer-global}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action ipv6-next-hop {[global ipv6-addr** <*next-hop-address*>**] | [local ipv6-addr** <*next-hop-address*>**] | peer-address | prefer-global}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
{[global ipv6-addr <*next-hop-address*>] | [**local ipv6-addr** <*next-hop-address*>] | **peer-address | prefer-global}**	Specifies the IPv6 address to be set as the next-hop address or peer address of the route .

Example

- Set the IP address of the peer address of the route with the value configured in the action clause.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action ipv6-next-hop peer-address
admin@Xorplus# commit
```

set routing route-map set-action label-index

The **set routing route-map set-action label-index** command modifies the label-index attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action label-index** command restores the default behavior of not modifying the label-index attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action label-index** <*label-index*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action label-index** <*label-index*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
label-index <*label-index*>	Specifies the label index value to be set in the route entry. Range: 0 to 1048560.

Example

- Configure a action clause in the route map to modify the label-index value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action label-index 100
admin@Xorplus# commit
```

set routing route-map set-action large-comm-list-delete

The **set routing route-map set-action large-comm-list-delete** command removes communities value from BGP large communities attribute.

When BGP route's communities value matches to the large community list name, the communities value is removed. When all of large communities value is removed eventually, the BGP update's large communities attribute is completely removed.

The **delete routing route-map set-action large-comm-list-delete** command restores the default behavior of not deleting the large community number attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action large-comm-list-delete** <*large-community-list*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action large-comm-list-delete** <*large-community-list*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
large-comm-list <*large-community-list*>	Specifies the name of the large-community-list.

Example

- Configure to remove communities value from BGP large communities attribute.

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action large-comm-list-delete LargeComlst
admin@Xorplus# commit
```

set routing route-map set-action local-preference

The **set routing route-map set-action local-preference** command modifies the local-preference attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action local-preference** command restores the default behavior of not modifying the local-preference attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action local-preference** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action local-preference** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
local-preference <*VALUE*>	Specifies the value to be set as the local-preference attribute of the route entry. Range: 0 to 4294967295.

Example

- Configure a action clause in the route map to modify the local-preference value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action local-preference 100
admin@Xorplus# commit
```

set routing route-map set-action metric

The **set routing route-map set-action metric** command modifies the metric attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action metric** command restores the default behavior of not modifying the metric attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action metric** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action metric** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
metric <*VALUE*>	Specifies the value to be set as the metric attribute of the route entry. Range: 0 to 4294967295.

Example

- Configure a action clause in the route map to modify the metric value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action metric 100
admin@Xorplus# commit
```

set routing route-map set-action metric-type

The **set routing route-map set-action metric-type** command modifies the metric-type attribute of the route entry with the value configured in the action clause. The **delete routing route-map set-action metric-type** command restores the default behavior of not modifying the metric-type attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action metric-type <type-1|type-2>**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action metric-type <type-1|type-2>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
metric-type <type-1|type-2>	Specifies the metric-type value of the route entry. The value could be **type-1** or **type-2**.

Example

- Configure a action clause in the route map to modify the metric-type value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action metric-type type-1
admin@Xorplus# commit
```

set routing route-map set-action origin

The **set routing route-map set-action origin** command modifies the origin attribute of the route entry with the value configured in the action clause.
The **delete routing route-map set-action origin** command restores the default behavior of not modifying the origin attribute of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action origin <egp|igp|incomplete>**

delete routing route-map <*route-map-name*>**order** <*NUMBER*> **set-action origin <egp|igp|incomplete>**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
origin <egp|igp|incomplete>	Selects the route update originated to IGP, EGP, or incomplete. When incomplete is selected, the route update origin is set to unknown.

Example

- Configure a action clause in the route map to modify the origin value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action origin egp
admin@Xorplus# commit
```

set routing route-map set-action originator-id

The **set routing route-map set-action originator-id** command modifies the originator-id attribute of the BGP route entry with the value configured in the action clause.
The **delete routing route-map set-action originator-id** command restores the default behavior of not modifying the originator-id attribute of the BGP route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action originator-id** <*ipv4-address*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action originator-id** <*ipv4-address*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
originator-id <*ipv4-address*>	Specifies originator-id attribute of the BGP route entry. The value is an IPv4 address.

Example

- Configure a action clause in the route map to modify the originator-id attribute of the BGP route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action originator-id 10.10.10.1
admin@Xorplus# commit
```

set routing route-map set-action src

The **set routing route-map set-action src** command sets the preferred source address for matching routes when installing in the kernel.
The **delete routing route-map set-action src** command restores the default behavior of not modifying the source address of the route entry.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action src {ipv4-addr** <*ipv4-address*>| **ipv6-addr** <*ipv6-address*>**}**

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action src {ipv4-addr** <ipv4-address>| **ipv6-addr**<ipv6-address>**}**

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
src {ipv4-addr <*ipv4-address*>| **ipv6-addr** <*ipv6-address*>**}**	Specifies the preferred source address to be set for a route.

Example

- Configure a action clause in the route map to modify the source address of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action src ipv4-addr 100.100.100.1
admin@Xorplus# commit
```

set routing route-map set-action tag

The **set routing route-map set-action tag** command modifies the tag value of the route with the one configured in the action clause. Applicable to static routes that will be redistributed to ospfv2 and ospfv3 protocols.
The **delete routing route-map set-action tag** command removes the action clause tag value.

Command Syntax

set routing route-map <*route-map-name***> order <***NUMBER***> set-action tag** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action tag** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
tag <*VALUE*>	Numeric value to change the route entry tag. Range: 0-65535. Required.

Example

- Configure a action clause in the route map to modify the tag value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action tag 100
admin@Xorplus# commit
```

set routing route-map set-action weight

The **set routing route-map set-action weight** command modifies the weight value of the route with the one configured in the action clause.
The **delete routing route-map set-action weight** command restores the default behavior of not modifying the weight attribute of the route.

Command Syntax

set routing route-map <*route-map-name***> order** <*NUMBER*>**set-action weight** <*VALUE*>

delete routing route-map <*route-map-name*> **order** <*NUMBER*> **set-action weight** <*VALUE*>

Parameter

Parameter	Description
route-map <*route-map-name***>**	Specifies the name of the route map. Required.
order <*NUMBER***>**	Specifies the sequence number of the entry. Required. The value is an integer that ranges from 1 to 65535.
weight <*VALUE*>	Specifies the value to be set as the weight attribute of the route. Range: 0 to 65535.

Example

- Configure a action clause in the route map to modify the weight value of the route:

```
admin@Xorplus# set routing route-map GlobalMap order 10 set-action weight 100
admin@Xorplus# commit
```

Route Leaking Commands

- BGP Route Leaking Commands
  - set protocols bgp ipv4-unicast import vrf
  - set protocols bgp ipv6-unicast import vrf
  - set protocols bgp ipv6-unicast import vrf-route-map
  - set protocols bgp vrf ipv4-unicast import vrf
  - set protocols bgp vrf ipv4-unicast import vrf-route-map
  - set protocols bgp vrf ipv6-unicast import vrf
- Static Route Leaking Commands
  - set protocols static route nexthop-vrf next-hop
  - set protocols static vrf route nexthop-vrf next-hop

BGP Route Leaking Commands

- set protocols bgp ipv4-unicast import vrf
- set protocols bgp ipv6-unicast import vrf
- set protocols bgp vrf ipv4-unicast import vrf
- set protocols bgp vrf ipv4-unicast import vrf-route-map
- set protocols bgp vrf ipv6-unicast import vrf

set protocols bgp ipv4-unicast import vrf

Run the command **set protocols bgp ipv4-unicast import vrf** to configure route leaking by importing BGP routes from the specified user defined non-default VRF into the default VRF.

Run the command **delete protocols bgp ipv4-unicast import vrf** to remove this configuration from the switch database.

Command Syntax

set protocols bgp ipv4-unicast import vrf <*vrf-name***>**

delete protocols bgp ipv4-unicast import vrf <*vrf-name***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF from which routes are imported. This is the destination VRF for the route and it must be a non-default user defined VRF. The value is a string.

Example

- This example configures route leaking by importing BGP routes from vrf2 into the default VRF.

```
admin@Xorplus# set protocols bgp ipv4-unicast import vrf vrf2
admin@Xorplus# commit
```

set protocols bgp ipv6-unicast import vrf

Run the command **set protocols bgp ipv6-unicast import vrf** to configure route leaking by importing IPv6 unicast routes from a user defined non-default VRF into the specified user defined VRF.

Run the command **delete protocols bgp ipv6-unicast import vrf** to delete this configuration from the switch database.

Command Syntax

set protocols bgp ipv6-unicast import vrf <*vrf-name***>**

delete protocols bgp ipv6-unicast import vrf <*vrf-name***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF from which routes are imported. This is must be a non-default user defined VRF. The value is a string.

Example

- This example configures route leaking by importing BGP IPv6 routes from vrf2 into the default VRF.

```
admin@Xorplus# set protocols bgp ipv6-unicast import vrf vrf2
admin@Xorplus# commit
```

set protocols bgp ipv6-unicast import vrf-route-map

Run the command **set protocols bgp ipv6-unicast import vrf-route-map** to specify a route map to filter IPv6 routes when importing routes from one VRF into another VRF. This command is useful to control the number of routes leaked between two VRFs using BGP. The conditions for which routes needs to be leaked and which routes should be excluded are specified in the route map and then applied when importing the routes. The optional parameter **vrf** is used to specify the VRF to which the routes are imported after filtering. If VRF is not specified then routes are imported into the default VRF.

Run the command **delete set protocols bgp ipv6-unicast import vrf-route-map** to delete this configuration from the switch database.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] ipv6-unicast import vrf-route-map <***map-name***>**

delete protocols bgp [vrf <*vrf-name***> ipv6-unicast import vrf-route-map**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Optional. Specifies the VRF name to which routes will be imported. The value is a string.
vrf-route-map <*map-name***>**	Specifies the name of the route map to apply when importing routes to a VRF. The value is a string.

Example

- This example applies route map *map1* when importing IPv6 routes into the default VRF.

```
admin@Xorplus# set protocols bgp ipv6-unicast import vrf-route-map map1
admin@Xorplus# commit
```

set protocols bgp vrf ipv4-unicast import vrf

Run the command **set protocols bgp vrf ipv4-unicast import vrf** to establish route leaking by importing IPv4 unicast routes from one VRF into another VRF.

Please note that the source VRF, to which the routes are imported to from the destination VRF must be a non-default VRF in this case. The destination VRF, from which the routes are imported can be a user defined non-default VRF or it could be the default VRF.

Run the command **delete protocols bgp vrf ipv4-unicast import vrf** to delete this configuration from the switch database.

Command Syntax

set protocols bgp vrf <*vrf-name***> ipv4-unicast import vrf <***vrf-name* **| default>**

delete protocols bgp vrf <*vrf-name***> ipv4-unicast import vrf <***vrf-name* **| default>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF name for the static route. This is the source VRF for the route and it must be a non-default user defined VRF. The value is a string.
vrf <*vrf-name* **| default>**	Specifies the destination VRF, it could be the default VRF or the user defined VRF. The value is a string.

Example

- This example configures route leaking by importing BGP IPv4 routes from vrf2 into vrf1.

```
admin@Xorplus# set protocols bgp vrf vrf1 ipv4-unicast import vrf vrf2
admin@Xorplus# commit
```

set protocols bgp vrf ipv4-unicast import vrf-route-map

Run the command **set protocols bgp ipv4-unicast import vrf-route-map** to specify a route map to filter IPv4 routes when importing routes from one VRF into another VRF. This command is useful to control the number of routes leaked between two VRFs using BGP. The conditions for which routes needs to be leaked and which routes should be excluded are specified in the route map and then applied when importing the routes. The optional parameter **vrf** is used to specify the VRF to which the routes are imported after filtering. If VRF is not specified then routes are imported into the default VRF.

Run the command **delete set protocols bgp ipv4-unicast import vrf-route-map** to delete this configuration from the switch database.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] ipv4-unicast import vrf-route-map <***map-name***>**

delete protocols bgp [vrf <*vrf-name***> ipv4-unicast import vrf-route-map**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Optional. Specifies the VRF name to which routes will be imported. The value is a string.
vrf-route-map <*map-name***>**	Specifies the name of the route map to apply when importing routes to a VRF. The value is a string.

Example

- This example applies route map *map1* when importing routes into the default VRF.

```
admin@Xorplus# set protocols bgp ipv4-unicast import vrf-route-map map1
admin@Xorplus# commit
```

set protocols bgp vrf ipv6-unicast import vrf

Run the command **set protocols bgp vrf ipv6-unicast import vrf** to enable route leaking by importing BGP IPv6 routes from the user defined or default VRF into the specified user defined non-default VRF.

Run the command **delete protocols bgp vrf ipv6-unicast import vrf** to delete this configuration from the switch database.

Command Syntax

set protocols bgp vrf <*vrf-name****> ipv6-unicast import vrf <****vrf-name*** **| default>**

delete protocols bgp vrf <*vrf-name****> ipv6-unicast import vrf <****vrf-name*** **| default>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the source VRF name for the imported IPv6 BGP route. This is the source VRF for the route and it must be a non-default user defined VRF. The value is a string.
vrf <*vrf-name* **| default>**	Specifies the destination VRF from which the routes are imported, it could be the default VRF or a user defined VRF. The value is a string.

Example

- This example configures route leaking by importing routes from vrf2 into vrf1.

```
admin@Xorplus# set protocols bgp vrf vrf1 ipv6-unicast import vrf vrf2
admin@Xorplus# commit
```

Static Route Leaking Commands

- set protocols static vrf route nexthop-vrf next-hop
- set protocols static route nexthop-vrf next-hop

set protocols static route nexthop-vrf next-hop

Run the command **set protocols static route nexthop-vrf next-hop** to configure a static leak route in the default VRF. The source VRF for the route is the default VRF and the destination next-hop router is in the specified next-hop VRF.

To delete this route, run the command **delete protocols static route nexthop-vrf.**

Command Syntax

set protocols static route <*IPv4Net* | *IPv6Net***> nexthop-vrf <***vrf-name***> next-hop <***IPv4* | *IPv6***>**

set protocols static route <*IPv4Net* | *IPv6Net***> nexthop-vrf <***vrf-name***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF name for the static route. This is the source VRF for the route.
route <*IPv4Net* | *IPv6Net***>**	Specifies the IPv4 or IPv6 network prefix, e.g. 10.0.0.0/24.
nexthop-vrf <*vrf-name***>**	Specifies the next-hop VRF for the static route. This is the destination VRF.
next-hop <*IPv4* | *IPv6***>**	Specifies the next-hop IPv4 or IPv6 router address in the destination VRF.

Usage Guidelines

Please note that if the route prefix chosen is an IPv4 network prefix then the next-hop router address in the next-hop VRF must also be an IPv4 address. Similarly, if the route prefix is an IPv6 network prefix, then the next-hop router address in the next-hop VRF must also be an IPv6 address.

Example

- Configure the static route leak in the default VRF for which the destination VRF is vrf2.

```
admin@Xorplus# set protocols static route 10.5.5.0/24 nexthop-vrf vrf2 next-hop 10.6.6.6
admin@Xorplus# commit
```

set protocols static vrf route nexthop-vrf next-hop

Run the command **set protocols static vrf route nexthop-vrf next-hop** to configure a static leak route. The route is created in one VRF for which the next-hop router is located in a different VRF.

Run the command **delete protocols static vrf route** to delete this static route the switch configuration.

Command Syntax

set protocols static vrf <*vrf-name***> route <***IPv4Net* **|** *IPv6Net***> nexthop-vrf <***vrf-name* **| default> next-hop <***IPv4* | *IPv6***>**

delete protocols static vrf <*vrf-name***> route <***IPv4Net* | *IPv6Net***>**

Parameter

Parameter	Description
vrf <*vrf-name***>**	Specifies the VRF name for the static route. This is the source VRF for the route.
route <*IPv4Net*	*IPv6Net***>**	Specifies the IPv4 or IPv6 network prefix, e.g. 10.0.0.0/24.
nexthop-vrf <*vrf-name***| default>**	Specifies the next-hop VRF for the static route. This is the destination VRF.
next-hop <*IPv4*	*IPv6***>**	Specifies the next-hop IPv4 or IPv6 router address in the destination VRF.

Usage Guidelines

Please note that if the route prefix chosen is an IPv4 network prefix then the next-hop router address in the next-hop VRF must also be an IPv4 address. Similarly, if the next route prefix is an IPv6 network prefix, then the next-hop router address in the next-hop VRF must also be an IPv6 address.

Example

- Configure the static route leak in vrf1 for which the destination VRF is vrf2.

```
admin@Xorplus# set protocols static vrf vrf1 route 10.5.5.0/24 nexthop-vrf vrf2 next-hop 10.6.6.6
admin@Xorplus# commit
```

BFD Configuration Commands

- run show bfd
- run show bfd counters
- run show bfd peers
- set protocols bfd multihop peer local-address
- set protocols bfd multihop peer local-address detect-multiplier
- set protocols bfd multihop peer local-address minimum-ttl
- set protocols bfd multihop peer local-address passive-mode
- set protocols bfd multihop peer local-address receive-interval
- set protocols bfd multihop peer local-address shutdown
- set protocols bfd multihop peer local-address transmit-interval
- set protocols bfd peer detect-multiplier
- set protocols bfd peer echo-mode
- set protocols bfd peer echo receive-interval
- set protocols bfd peer echo transmit-interval
- set protocols bfd peer local-address
- set protocols bfd peer minimum-ttl
- set protocols bfd peer passive-mode
- set protocols bfd peer receive-interval
- set protocols bfd peer shutdown
- set protocols bfd peer transmit-interval
- set protocols bfd profile
- set protocols bfd profile detect-multiplier
- set protocols bfd profile echo-mode
- set protocols bfd profile echo receive-interval
- set protocols bfd profile echo transmit-interval
- set protocols bfd profile minimum-ttl
- set protocols bfd profile passive-mode
- set protocols bfd profile receive-interval
- set protocols bfd profile shutdown
- set protocols bfd profile transmit-interval
- set protocols bgp bfd
- set protocols ospf6 interface bfd
- set protocols ospf interface bfd
- set protocols pim interface bfd

run show bfd

The **run show bfd** command displays informations about BFD.

Command Syntax

run show bfd [**vrf** <*vrf-name*>] [**interface** <*interface*>] | **multihop**] ***peer*** <*peer-ip*> [**local-address** <*local-ip*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
[**interface** <*interface*>] | **multihop**]	Optional. • **interface** <*interface*>: Specifies an interface for BGP connection. • **multihop**: Shows informations about a multi-hop BFD session.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Optional. Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address. **Note:** This option is mandatory for IPv6.

Example

• Show information about the BFD session.

```
admin@Xorplus# run show bfd peer 1.1.1.1
BFD Peer:
        peer 1.1.1.1 local-address 1.1.1.2 vrf default
                ID: 531846395
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 2
                        Receive interval: 50ms
                        Transmission interval: 50ms
                        Echo receive interval: disabled
                        Echo transmission interval: 10ms
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
                        Echo receive interval: disabled

admin@Xorplus# run show bfd interface vlan3 peer 1.1.1.1
BFD Peer:
        peer 1.1.1.1 local-address 1.1.1.2 vrf default
                ID: 531846395
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 2
                        Receive interval: 50ms
                        Transmission interval: 50ms
```

```
                        Echo receive interval: disabled
                        Echo transmission interval: 10ms
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
                        Echo receive interval: disabled


admin@Xorplus# run show bfd interface vlan3 peer 1.1.1.1 local-address 1.1.1.2
BFD Peer:
        peer 1.1.1.1 local-address 1.1.1.2 vrf default
                ID: 531846395
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 2
                        Receive interval: 50ms
                        Transmission interval: 50ms
                        Echo receive interval: disabled
                        Echo transmission interval: 10ms
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
                        Echo receive interval: disabled

admin@Xorplus# run show bfd multihop peer 1.1.1.1
BFD Peer:
        peer 1.1.1.1 multihop local-address 1.1.1.2 vrf default
                ID: 868601837
                Remote ID: 0
                Active mode
                Minimum TTL: 254
                Status: down
                Downtime: 1 hour(s), 52 minute(s), 15 second(s)
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 3
                        Receive interval: 300ms
                        Transmission interval: 300ms
                        Echo receive interval: 50ms
                        Echo transmission interval: disabled
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
                        Echo receive interval: disabled


admin@Xorplus# run show bfd vrf vrf1 peer 1.1.1.1
BFD Peer:
        peer 1.1.1.1 local-address 1.1.1.2 vrf vrf1
                ID: 2172419937
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 2
                        Receive interval: 50ms
                        Transmission interval: 50ms
```

```
        Echo receive interval: disabled
        Echo transmission interval: 10ms
Remote timers:
        Detect-multiplier: 3
        Receive interval: 1000ms
        Transmission interval: 1000ms
        Echo receive interval: disabled
```

run show bfd counters

The **run show bfd** command displays the counter informations about BFD sessions.

Command Syntax

run show bfd [**vrf** <*vrf-name*>] [**interface** <*interface*>] | **multihop**] ***peer*** <*peer-ip*> **counters**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
[**interface** <*interface*>] | **multihop**]	Optional. • **interface** <*interface*>: Specifies an interface for BGP connection. • **multihop**: Shows informations about a multi-hop BFD session.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Example
• Show the counter information about the BFD session.

```
admin@Xorplus# run show bfd peer 1.1.1.1 counters
peer 1.1.1.1 local-address 1.1.1.2 vrf default
                Control packet input: 0 packets
                Control packet output: 1 packets
                Echo packet input: 0 packets
                Echo packet output: 0 packets
                Session up events: 0
                Session down events: 0
                Zebra notifications: 1
```

run show bfd peers

The **run show bfd peers** command displays informations about all the BFD sessions.

Command Syntax

run show bfd [**vrf** <*vrf-name*>] **peers [brief | counters]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
[brief | counters]	Optional. • **brief**: Displays brief information about all the BFD sessions. • **counters**: Displays the counter information about all the BFD sessions.

Example

• Show information about all the BFD session.

```
admin@Xorplus# run show bfd peers
BFD Peers:
        peer 3.3.3.3 local-address 3.3.3.2 vrf vrf1 interface vlan100
                ID: 984327
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 20
                        Receive interval: 50ms
                        Transmission interval: 50ms
                        Echo receive interval: 30ms
                        Echo transmission interval: 30ms
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
                        Echo receive interval: disabled

        peer 3.3.3.3 local-address 3.3.3.2 vrf default interface vlan3
                ID: 3820553826
                Remote ID: 0
                Passive mode
                Status: shutdown
                Diagnostics: ok
                Remote diagnostics: ok
                Peer Type: configured
                Local timers:
                        Detect-multiplier: 2
                        Receive interval: 50ms
                        Transmission interval: 50ms
                        Echo receive interval: 10ms
                        Echo transmission interval: 10ms
                Remote timers:
                        Detect-multiplier: 3
                        Receive interval: 1000ms
                        Transmission interval: 1000ms
```

```
                Echo receive interval: disabled

peer 2.2.2.2 multihop local-address 2.2.2.3 vrf vrf1
        ID: 219448436
        Remote ID: 0
        Active mode
        Minimum TTL: 254
        Status: down
        Downtime: 1 hour(s), 53 minute(s), 4 second(s)
        Diagnostics: ok
        Remote diagnostics: ok
        Peer Type: configured
        Local timers:
                Detect-multiplier: 3
                Receive interval: 300ms
                Transmission interval: 300ms
                Echo receive interval: 50ms
                Echo transmission interval: disabled
        Remote timers:
                Detect-multiplier: 3
                Receive interval: 1000ms
                Transmission interval: 1000ms
                Echo receive interval: disabled
```

set protocols bfd multihop peer local-address

The **set protocols bfd multihop peer local-address** command creates a multi-hop BFD session and specifies the peer IP address.

The **delete protocols bfd multihop peer local-address** command deletes the multi-hop BFD session.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] ***peer*** <*peer-ip*> [**local-address** <*local-ip*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Optional. Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address. **Note:** This option is mandatory for IPv6.

Example

- Create a multi-hop BFD session to the peer IP address 2.2.2.2.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address detect-multiplier

The **set protocols bfd multihop peer local-address detect-multiplier** command configures the detection multiplier to determine packet loss for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address detect-multiplier** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **detect-multiplier <***MULTIPLIER***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
detect-multiplier <*MULTIPLIER***>**	Specifies the BFD detection multiplier. The value is an integer that ranges from 2 to 255. The default value is 3.

Usage Guidelines

The remote transmission interval will be multiplied by this value to determine the connection loss detection timer.

Example: when the local system has *detect-multiplier* 3 and the remote system has *transmission interval* 300, the local system will detect failures only after 900 milliseconds without receiving packets.

Example

- Configure the BFD detection multiplier to 4 for BFD peer 2.2.2.2 for a multi-hop BFD session.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 detect-multiplier 4
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address minimum-ttl

The **set protocols bfd multihop peer local-address minimum-ttl** command configures the minimum expected TTL for an incoming BFD control packet for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address minimum-ttl** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **minimum-ttl <***minimum-ttl***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
minimum-ttl <*minimum-ttl***>**	Specifies the minimum expected TTL. Range: 1 to 254.

Usage Guidelines

This feature serves the purpose of thightening the packet validation requirements to avoid receiving BFD control packets from other sessions.

Note that: This feature is for multi-hop sessions only.

Example

- Configure the minimum expected TTL to 252.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 minimum-ttl 252
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address passive-mode

The **set protocols bfd multihop peer local-address passive-mode** command configures the BFD session as passive for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address passive-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **passive-mode**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.

Usage Guidelines

A passive session will not attempt to start the connection and will wait for control packets from peer before it begins replying.
This feature is useful when you have a router that acts as a central node in a star network and you want to avoid all the other nodes sending BFD control packets.

Example

- Configure the BFD session as passive.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 passive-mode
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address receive-interval

The **set protocols bfd multihop peer local-address receive-interval** command configures the minimum interval that this system is capable of receiving control packets for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **receive-interval <***receive-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
receive-interval <*receive-interval***>**	Specifies the minimum receive interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum receive interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 receive-interval 500
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address shutdown

The **set protocols bfd multihop peer local-address shutdown** command can be used to disable the BFD peer. When the peer is disabled an ‘administrative down’ message is sent to the remote peer for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address shutdown** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It’s a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.

Example

- Disable the BFD peer.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3shutdown
admin@Xorplus# commit
```

set protocols bfd multihop peer local-address transmit-interval

The **set protocols bfd multihop peer local-address transmit-interval** command configures the minimum transmission interval (less jitter) that this system wants to use to send BFD control packets for a multi-hop BFD session.

The **delete protocols bfd multihop peer local-address transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd multihop [**vrf** <*vrf-name*>] **peer**<*peer-ip*> **local-address** <*local-ip*> **transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address.
transmit-interval <*transmit-interval***>**	Specifies the minimum transmission interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum transmission interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd multihop peer 2.2.2.2 local-address 2.2.2.3 transmit-interval 500
admin@Xorplus# commit
```

set protocols bfd peer detect-multiplier

The **set protocols bfd peer detect-multiplier** command configures the detection multiplier to determine packet loss for a single-hop BFD session.

The **delete protocols bfd peer detect-multiplier** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **detect-multiplier <***MULTIPLIER***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
detect-multiplier <*MULTIPLIER***>**	Specifies the BFD detection multiplier. The value is an integer that ranges from 2 to 255. The default value is 3.

Usage Guidelines

The remote transmission interval will be multiplied by this value to determine the connection loss detection timer.

Example: when the local system has *detect-multiplier* 3 and the remote system has *transmission interval* 300, the local system will detect failures only after 900 milliseconds without receiving packets.

Example

- Configure the BFD detection multiplier to 4 for BFD peer 2.2.2.2.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 detect-multiplier 4
admin@Xorplus# commit
```

set protocols bfd peer echo-mode

The **set protocols bfd peer echo-mode** command can be used to enable BFD echo mode for a single-hop BFD session. This mode is disabled by default.

The **delete protocols bfd peer echo-mode** command sets the configuration to the default value.

NOTEs:
- Echo function is only supported in single-hop BFD case.
- BFD echo mode is incompatible with that on other vendors, that is, echo mode can work only between PICOS switches.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **echo-mode**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Usage Guidelines

It is recommended that the transmission interval of control packets to be increased after enabling echo-mode to reduce bandwidth usage. For example: transmit-interval 2000.
Echo mode is not supported on multi-hop setups.

Example

- Enable BFD echo mode for BFD peer 2.2.2.2.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 echo-mode
admin@Xorplus# commit
```

set protocols bfd peer echo receive-interval

The **set protocols bfd peer echo receive-interval** command configures the minimum time interval between received BFD echo packets for a single-hop BFD session.

The **delete protocols bfd peer echo receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **echo receive-interval** [**<***receive-interval***> | disabled**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
echo receive-interva [**<***receive-interval***>	disabled**]	Specifies the minimum time interval between received BFD echo packets in milliseconds. The value **disabled** indicates that the switch does not support reception of BFD echo packets. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between received BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 echo receive-interval 60
admin@Xorplus# commit
```

set protocols bfd peer echo transmit-interval

The **set protocols bfd peer echo transmit-interval** command configures the minimum time interval between transmitted BFD echo packets for a single-hop BFD session.

The **delete protocols bfd peer echo transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **echo transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
echo transmit-interval <*transmit-interval***>**	Specifies the minimum time interval between transmitted BFD echo packets in milliseconds. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between transmitted BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 echo transmit-interval 60
admin@Xorplus# commit
```

set protocols bfd peer local-address

The **set protocols bfd peer local-address** command creates a BFD session and specifies the peer IP address.

The **delete protocols bfd peer local-address** command delete the BFD session.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer*** <*peer-ip*> [**local-address** <*local-ip*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
local-address <*local-ip*>	Specifies a local address used to send the packets. The value is an IPv4 or IPv6 address. **Note:** This option is mandatory for IPv6.

Example

- Create a BFD session link to the peer IP address 2.2.2.2.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2
admin@Xorplus# commit
```

set protocols bfd peer minimum-ttl

The **set protocols bfd peer minimum-ttl** command configures the minimum expected TTL for an incoming BFD control packet for a single-hop BFD session.

The **delete protocols bfd peer minimum-ttl** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **minimum-ttl <***minimum-ttl***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
minimum-ttl <*minimum-ttl***>**	Specifies the minimum expected TTL. Range: 1 to 254.

Usage Guidelines

This feature serves the purpose of tightening the packet validation requirements to avoid receiving BFD control packets from other sessions.

Note that: This feature is for multi-hop sessions only.

Example

- Configure the minimum expected TTL to 252.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 minimum-ttl 252
admin@Xorplus# commit
```

set protocols bfd peer passive-mode

The **set protocols bfd peer passive-mode** command configures the BFD session as passive for a single-hop BFD session.

The **delete protocols bfd peer passive-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **passive-mode**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Usage Guidelines

A passive session will not attempt to start the connection and will wait for control packets from peer before it begins replying.
This feature is useful when you have a router that acts as a central node in a star network and you want to avoid other nodes sending BFD control packets proactively.

Example

- Configure the BFD session as passive.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 passive-mode
admin@Xorplus# commit
```

set protocols bfd peer receive-interval

The **set protocols bfd peer receive-interval** command configures the minimum interval that this system is capable of receiving control packets for a single-hop BFD session.

The **delete protocols bfd peer receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **receive-interval <***receive-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
receive-interval <*receive-interval***>**	Specifies the minimum receive interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum receive interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 receive-interval 500
admin@Xorplus# commit
```

set protocols bfd peer shutdown

The **set protocols bfd peer shutdown** command can be used to disable the BFD peer for a single-hop BFD session. When the peer is disabled an 'administrative down' message is sent to the remote peer.

The **delete protocols bfd peer shutdown** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **shutdown**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.

Example

- Disable the BFD peer.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 shutdown
admin@Xorplus# commit
```

set protocols bfd peer transmit-interval

The **set protocols bfd peer transmit-interval** command configures the minimum transmission interval (less jitter) that this system wants to use to send BFD control packets for a single-hop BFD session.

The **delete protocols bfd peer transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd [**vrf** <*vrf-name*>] [**interface**<*interface-name*>] ***peer***<*peer-ip*> **transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
interface<*interface-name*>	Optional. Specifies the egress interface for BFD packets. The value is an L3 interface that can be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string. If not specified, the system will search the route table for the outgoing interface.
peer <*peer-ip*>	Specifies the peer for a BFD session. The value is an IPv4 or IPv6 address.
transmit-interval <*transmit-interval***>**	Specifies the minimum transmission interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum transmission interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd peer 2.2.2.2 transmit-interval 500
admin@Xorplus# commit
```

set protocols bfd profile

The **set protocols bfd profile** command adds a new profile for OSPFv2/v3, BGP or PIM protocols to modify the BFD parameters.

The **delete protocols bfd profile** command deletes the profile.

Command Syntax

set protocols bfd profile <*profile-name*>

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.

Example

- Creates a BFD profile p2.

```
admin@Xorplus# set protocols bfd profile p2
admin@Xorplus# commit
```

set protocols bfd profile detect-multiplier

The **set protocols bfd profile detect-multiplier** command configures the detection multiplier to determine packet loss for a profile.

The **delete protocols bfd profile detect-multiplier** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile *<profile-name>* **detect-multiplier <***MULTIPLIER***>**

Parameter

Parameter	Description
profile *<profile-name>*	Specifies the profile name. The value is a string.
detect-multiplier <*MULTIPLIER***>**	Specifies the BFD detection multiplier. The value is an integer that ranges from 2 to 255. The default value is 3.

Usage Guidelines

The remote transmission interval will be multiplied by this value to determine the connection loss detection timer.

Example: when the local system has *detect-multiplier* 3 and the remote system has *transmission interval* 300, the local system will detect failures only after 900 milliseconds without receiving packets.

Example

- Configure the BFD detection multiplier to 4 for profile p2.

```
admin@Xorplus# set protocols bfd profile p2 detect-multiplier 4
admin@Xorplus# commit
```

set protocols bfd profile echo-mode

The **set protocols bfd profile echo-mode** command can be used to enable BFD echo mode for a profile. This mode is disabled by default.

The **delete protocols bfd profile echo-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile *<profile-name>* **echo-mode**

Parameter

Parameter	Description
profile *<profile-name>*	Specifies the profile name. The value is a string.

Usage Guidelines

It is recommended that the transmission interval of control packets to be increased after enabling echo-mode to reduce bandwidth usage. For example: transmit-interval of 2000ms.
Echo mode is not supported on multi-hop BFD sessions.

Example

- Enable BFD echo mode.

```
admin@Xorplus# set protocols bfd profile p2 echo-mode
admin@Xorplus# commit
```

set protocols bfd profile echo receive-interval

The **set protocols bfd profile echo receive-interval** command configures the minimum time interval between received BFD echo packets for a profile.

The **delete protocols bfd profile echo receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **echo receive-interval** [**<***receive-interval***> | disabled**]

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
echo receive-interva [**<***receive-interval***> | disabled**]	Specifies the minimum time interval between received BFD echo packets in milliseconds. The value **disabled** indicates that the switch does not support reception of BFD echo packets. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between received BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 echo receive-interval 60
admin@Xorplus# commit
```

set protocols bfd profile echo transmit-interval

The **set protocols bfd profile echo transmit-interval** command configures the minimum time interval between transmitted BFD echo packets for a profile.

The **delete protocols bfd profile echo transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **echo transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
echo transmit-interval <*transmit-interval***>**	Specifies the minimum time interval between transmitted BFD echo packets in milliseconds. Range: 10 to 60000. Default: 50ms.

Example

- Configure the minimum time interval between transmitted BFD echo packets to 60 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 echo transmit-interval 60
admin@Xorplus# commit
```

set protocols bfd profile minimum-ttl

The **set protocols bfd profile minimum-ttl** command configures the minimum expected TTL for an incoming BFD control packet for a profile.

The **delete protocols bfd profile minimum-ttl** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **minimum-ttl <***minimum-ttl***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
minimum-ttl <*minimum-ttl***>**	Specifies the minimum expected TTL. Range: 1 to 254.

Usage Guidelines

This feature serves the purpose of tightening the packet validation requirements to avoid receiving BFD control packets from other sessions.

Note that: This feature is for multi-hop sessions only.

Example

- Configure the minimum expected TTL to 252.

```
admin@Xorplus# set protocols bfd profile p2 minimum-ttl 252
admin@Xorplus# commit
```

set protocols bfd profile passive-mode

The **set protocols bfd profile passive-mode** command configures the BFD session as passive for a profile.

The **delete protocols bfd profile passive-mode** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **passive-mode**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.

Usage Guidelines

A passive session will not attempt to start the connection and will wait for control packets from peers before it begins replying.
This feature is useful when you have a router that acts as a central node in a star network and you want to avoid other BFD nodes sending control packets proactively.

Example

- Configure the BFD session as passive.

```
admin@Xorplus# set protocols bfd profile p2 passive-mode
admin@Xorplus# commit
```

set protocols bfd profile receive-interval

The **set protocols bfd profile receive-interval** command configures the minimum interval that this system is capable of receiving control packets for a profile.

The **delete protocols bfd profile receive-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **receive-interval <***receive-interval***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
receive-interval <*receive-interval***>**	Specifies the minimum receive interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum receive interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 receive-interval 500
admin@Xorplus# commit
```

set protocols bfd profile shutdown

The **set protocols bfd profile shutdown** command can be used to disable a BFD peer. When the peer is disabled an ‘administrative down’ message is sent to the remote peer for a profile.

The **delete protocols bfd profile shutdown** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **shutdown**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.

Example

- Disable the BFD peer.

```
admin@Xorplus# set protocols bfd profile p2 shutdown
admin@Xorplus# commit
```

set protocols bfd profile transmit-interval

The **set protocols bfd profile transmit-interval** command configures the minimum transmission interval (less jitter) that this system wants to use to send BFD control packets for a profile.

The **delete protocols bfd profile transmit-interval** command sets the configuration to the default value.

Command Syntax

set protocols bfd profile <*profile-name*> **transmit-interval <***transmit-interval***>**

Parameter

Parameter	Description
profile <*profile-name*>	Specifies the profile name. The value is a string.
transmit-interval <*transmit-interval***>**	Specifies the minimum transmission interval in milliseconds. Range: 300 to 60000. Default: 300ms.

Example

- Configure the minimum transmission interval to 500 milliseconds.

```
admin@Xorplus# set protocols bfd profile p2 transmit-interval 500
admin@Xorplus# commit
```

set protocols bgp bfd

The **set protocols bgp bfd** command enables BFD for BGP.
The **delete protocols bgp bfd** command disables this feature.

Command Syntax

set protocols bgp [**vrf** <*vrf-name*>] **{neighbor** <*ip*>**| peer-group** <*peer-group*> |**interface** <*interface*>**} bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
neighbor <*ip*>	Specifies the IP address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** can be used to modify parameters for a BFD session.

Example
• Enable BFD for BGP.

```
admin@XorPlus# set protocols bgp neighbor 2.2.2.2 bfd
admin@XorPlus# commit
```

set protocols ospf6 interface bfd

Run the command **set protocols ospf6 interface bfd** to enable BFD for OSPFv3 on the L3 interface.

Run the command **delete protocols ospf6 interface bfd** to remove this configuration.

Command Syntax

set protocols ospf6 interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

delete protocols ospf6 interface <*interface-name***> bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** can be used to modify parameters for BFD session.

Example

- Enable BFD for OSPFv3 on the VLAN interface.

```
admin@XorPlus# set protocols ospf6 interface vlan200
admin@Xorplus# commit
```

set protocols ospf interface bfd

Run the command **set protocols ospf interface bfd** to enable BFD for OSPFv2 on the L3 interface.

Run the command **delete protocols ospf interface bfd** to remove this configuration.

Command Syntax

set protocols ospf interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

delete protocols ospf interface <*interface-name***> bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** name can be used to modify parameters for BFD session.

Example

- Enable BFD for OSPFv2 on the VLAN interface.

```
admin@XorPlus# set protocols ospf interface vlan200 bfd
admin@Xorplus# commit
```

set protocols pim interface bfd

Run the command **set protocols pim interface bfd** to enables BFD for PIM on the L3 interface.

Run the command **delete protocols pim interface bfd** to remove this configuration.

Command Syntax

set protocols pim interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

delete protocols pim interface <*interface-name*> **bfd** [**profile** <*profile-name*>]

Parameter

Parameter	Description
interface <*vlan-interface*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
profile <*profile-name*>	Optional. Specifies the profile name. The value is a string. It has to be pre-defined by the command **set protocols bfd profile xx**. **Profile** name can be used to modify parameters for BFD session.

Example

- Enable BFD for PIM on the VLAN interface.

```
admin@XorPlus# set protocols pim interface vlan200 bfd
admin@Xorplus# commit
```

Policy-Based Routing (PBR) Commands

- set routing pbr map sequence match destination-ipv4
- set routing pbr map sequence match source-ipv4
- set routing pbr map sequence match destination-port
- set routing pbr map sequence match source-port
- set routing pbr map sequence match destination-ipv6
- set routing pbr map sequence match source-ipv6
- set routing pbr map sequence action nexthop
- set routing pbr map sequence action dscp
- set routing pbr map vlan-interface
- run show pbr map
- run clear pbr map

set routing pbr map sequence match destination-ipv4

The **set routing pbr map sequence match destination-ipv4** command configures a match rule based on the destination IPv4 address for PBR traffic classification.

The **delete routing pbr map sequence match destination-ipv4** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-ipv4** <*ipv4-address/*prefix-length>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match destination-ipv4**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
destination-ipv4 <*ipv4-address/prefix-length*>	Specifies destination IPv4 address, it should be an IPv4 subnet in the format of IPv4-address/prefix-length. For example, 10.1.1.0/24, 192.168.10.10/32.

Example

- Configure a match rule based on the destination IPv4 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match destination-ipv4 10.1.1.0/24
admin@PICOS# commit
```

set routing pbr map sequence match source-ipv4

The **set routing pbr map sequence match source-ipv4** command configures a match rule based on the source IPv4 address for PBR traffic classification.

The **delete routing pbr map sequence match source-ipv4** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv4** <*ipv4-address/prefix-length*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match source-ipv4**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
source-ipv4 <*ipv4-address/prefix-length*>	Specifies source IPv4 address, it should be an IPv4 subnet in the format of IPv4-address/prefix-length. For example, 10.1.1.0/24.

Example

- Configure a match rule based on the source IPv4 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match source-ipv4 10.1.1.0/24
admin@PICOS# commit
```

set routing pbr map sequence match destination-port

The **set routing pbr map sequence match destination-port** command configures a match rule based on the destination port for PBR traffic classification.

The **delete routing pbr map sequence match destination-port** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-port** <*destination-port*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match destination-port**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
destination-port <*destination-port*>	Specifies the destination port number. The value is an integer that ranges from 1 to 65535.

Example

- Configure a match rule based on the destination port for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match destination-port 7000
admin@PICOS# commit
```

set routing pbr map sequence match source-port

The **set routing pbr map sequence match source-port** command configures a match rule based on the source port for PBR traffic classification.

The **delete routing pbr map sequence match source-port** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-port** <*source-port*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match source-port**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
source-port <*source-port*>	Specifies the source port number. The value is an integer that ranges from 1 to 65535.

Example

- Configure a match rule based on the source port for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match source-port 7035
admin@PICOS# commit
```

set routing pbr map sequence match destination-ipv6

The **set routing pbr map sequence match destination-ipv6** command configures a match rule based on the destination IPv6 address for PBR traffic classification.

The **delete routing pbr map sequence match destination-ipv6** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match destination-ipv6** <*ipv6-address/prefix-length*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **match destination-ipv6**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
destination-ipv6 <*ipv6-address/prefix-length*>	Specifies destination IPv6 address, it should be an IPv6 subnet in the format of IPv6-address/prefix-length. For example, 2001::0/32.

Example

- Configure a match rule based on the destination IPv6 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match destination-ipv6 2001::0/64
admin@PICOS# commit
```

set routing pbr map sequence match source-ipv6

The **set routing pbr map sequence match source-ipv6** command configures a match rule based on the source IPv6 address for PBR traffic classification.

The **delete routing pbr map sequence match source-ipv6** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv6** <*ipv6-address/prefix-length*>

delete routing pbr map <*map-name*> **sequence** <*sequence-number*> **match source-ipv6**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
source-ipv6 <*ipv6-address/prefix-length*>	Specifies source IPv6 address, it should be an IPv6 subnet in the format of IPv6-address/prefix-length. For example, 2001::0/32.

Example

- Configure a match rule based on the source IPv6 address for PBR traffic classification.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 match source-ipv6 2001:a100::0/64
admin@PICOS# commit
```

set routing pbr map sequence action nexthop

The **set routing pbr map sequence action nexthop** command configures an action to redirect packets to a next-hop IP address for policy-based routing. The next-hop address must be directly connected and reachable without supporting recursion.

The **delete routing pbr map sequence action nexthop** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action nexthop** <*ip-address*> [**nexthop-vrf** <*vrf-name*>]

delete routing pbr map <*map-name*> **sequence** <*sequence-number*> **match action nexthop** <*ip-address*> [**nexthop-vrf**]

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
nexthop <*ip-address*>	Specifies next-hop IP, it could be a specific IPv4/IPv6 address. For example, 192.168.1.10.
nexthop-vrf <*vrf-name*>	Optional. Specifies the name of the VRF for the next-hop route. • When a VRF name is specified, find the next hop routing information from the specified VRF domain. • When no VRF is specified, find the next hop routing information from the default VRF.

Example

- Configure an action to redirect packets to a next-hop IP address for policy-based routing.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 action nexthop 10.30.1.10
admin@PICOS# commit
```

set routing pbr map sequence action dscp

The **set routing pbr map sequence action dscp** command configures an action to modify the DSCP value in packets for policy-based routing.

The **delete routing pbr map sequence action dscp** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **sequence** <*sequence-number*> **action dscp** <*dscp-value*>

delete routing pbr map <*map-name*>**sequence** <*sequence-number*> **action dscp**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
sequence <*sequence-number*>	Specifies sequence number. The value is an integer that ranges from 1 to 700.
dscp <*dscp-value*>	Specifies a value to modify the DSCP value in packets. The value is an integer in the range of 0 to 63.

Example

- Configure an action to modify the DSCP value in packets for policy-based routing.

```
admin@PICOS# set routing pbr map PBR_map1 sequence 100 action dscp 40
admin@PICOS# commit
```

set routing pbr map vlan-interface

The **set routing pbr map vlan-interface** command applies the PBR policy to the VLAN interface where the traffic is coming in.

The **delete routing pbr map vlan-interface** command deletes the configuration.

Command Syntax

set routing pbr map <*map-name*> **vlan-interface** <*vlan-interface*>

delete routing pbr map <*map-name*> **vlan-interface**

Parameter

Parameter	Description
map <*map-name*>	Specifies the map name of a PBR policy. The value is a string.
vlan-interface <*vlan-interface*>	Specifies the VLAN interface name. The value is a string.

Example

- Apply the PBR policy on a VLAN interface.

```
admin@PICOS# set routing pbr map PBR_map1 vlan-interface vlan100
admin@PICOS# commit
```

run show pbr map

The **run show pbr map** command shows the configuration information of policy-based routing.

Command Syntax

run show pbr map [<*map-name*>]

Parameter

Parameter	Description
<*map-name*>	Optional. Specifies the map name of a PBR policy. The value is a string.

Example

- View the configuration information of policy-based routing.

```
admin@PICOS# run show pbr map
pbr-map        l3-interface
-----------    -------------
map1           vlan20

admin@PICOS# run show pbr map map1
Sequence: 1
    match-condition:
        destination-ipv4      1.1.1.0/24
    action:
        nexthop:20.0.0.1 nexthop-vrf:
    statistics:
        vlan2: 0 pkts

```

run clear pbr map

The **run show pbr map** command clears the statistics information of a PBR map.

> **NOTE:**
>
> The previous statistics cannot be restored after clearing, so be careful when using this command.

Command Syntax

run show pbr map <**all** | <*map-name*> [**sequence** <*sequence-number*>]>

Parameter

Parameter	Description
all | <*map-name*>	Specifies the map name of a PBR policy. The value is a string. When **all** is specified, clear the statistics information of all PBR maps.
sequence <*sequence-number*>	Optional. Specifies sequence number. The value is an integer that ranges from 1 to 700.

Example

- Clear the statistics information of a PBR map.

```
admin@PICOS# run clear pbr map map1
Pbr map statistics cleared.

admin@PICOS# run clear pbr map all
Pbr map statistics cleared.
```

IPv4 Source Guard (IPSG for IPv4) Commands

- set ip-source-guard binding ip
- set ip-source-guard enable
- set ip-source-guard verify
- set ip-source-guard traceoptions enable
- run show ip-source-guard binding

set ip-source-guard binding ip

The **set ip-source-guard binding ip** command configures a static IP source guard binding entry.

The **delete ip-source-guard binding ip** command deletes the configuration.

Command Syntax

set ip-source-guard binding ip <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*>

delete ip-source-guard binding ip<*ip_address*> [**mac** <*mac-address*> **interface**<*interface-name*>**vlan** <*vlan-id*>]

Parameter

Parameter	Description
ip <*ip_address*>	Specifies a source IPv4 address for the static binding entry. The IPv4 address must be a class A, B, or C address, and cannot be 127.x.x.x, 0.0.0.0, or a multicast IP address.
mac <*mac-address*>	Specifies a source MAC address for the static binding entry. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers, and cannot be all 0s, all Fs (a broadcast address), or a multicast address.
interface <*interface-name*>	Specifies ingress interface name for the static binding entry. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IP source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

In IP Source Guard, static binding entries involve manually associating IP addresses with specific interfaces on a network device. IP Source Guard allows only traffic with matching source IP addresses and source MAC addresses to pass through the specified interface, thereby enhancing network security by preventing IP address spoofing attacks.

NOTE:

In the following example, a static IP source guard binding entry is configured on the device. When attempting to delete this entry, an error occurs.

```
set ip-source-guard binding ip 110.100.10.2 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10

admin@PICOS# delete ip-source-guard binding ip 110.100.10.2 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10
Deleting:
  10
```

```
OK
admin@PICOS# commit
IPSG: vlan is required for ip 110.100.10.2, mac 00:00:00:00:00:01, interface ge-1/1/1
Commit failed.

admin@PICOS# delete ip-source-guard binding ip 110.100.10.2 mac 00:00:00:00:00:01
Deleting:
    00:00:00:00:00:01 {
                interface "ge-1/1/1" {
                    vlan 10
        }
    }
OK
admin@PICOS# commit
IPSG: mac is required for ip 110.100.10.2
Commit failed.
```

This is typically caused by the following two reasons:

- Due to the hierarchy structure design of PICOS CLI, when performing a deletion operation, the specified level and all its subordinate levels (i.e., the parameters and subsequent parameters in the command line) will be deleted, while the upper-level hierarchy (i.e., the parameters before the command line) will not be deleted.
- In the configuration of a static IP source guard binding entry, the command **set ip-source-guard binding ip** <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*> requires all four parameters: IP address, MAC address, interface name, and VLAN ID, to be configured.

For this type of deletion error, you can complete the deletion configuration by removing the first hierarchy level **ip-source-guard binding ip**.

```
admin@PICOS# delete ip-source-guard binding ip 110.100.10.2
Deleting:
    110.100.10.2 {
        mac 00:00:00:00:00:01 {
            interface "ge-1/1/1" {
                vlan 10
            }
        }
    }
OK

admin@PICOS# commit
Commit OK.
Save done.
```

Example

- Configure a static IP source guard binding entry manually.

```
admin@PICOS# set ip-source-guard binding ip 10.1.1.10 mac 22:22:22:11:11:11 interface ge-1/1/3 vlan 40
admin@PICOS# commit
```

set ip-source-guard enable

The **set ip-source-guard enable** command can be used to enable or disable IP source guard function based on ingress interface and VLAN of the packet.

The **delete ip-source-guard enable** command deletes the configuration.

Command Syntax

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true | false**>

delete ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IP source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IP source guard static binding table, specifies the VLAN ID manually configured in IP source guard static binding table. • For IP source guard dynamic binding table, specifies the VLAN ID enabled DHCP snooping.
enable <**true	false**>	Enable or disable IP source guard function. The value could be **true** or **false**. • **true**: Enable IP source guard function. • **false**: Disable IP source guard function. By default, IP source guard function is disabled.

Usage Guidelines

IP source guard should be enabled based on specific interfaces and VLANs. When IP source guard is enabled based on a specific interface and VLAN, all packets from that interface and VLAN will be dropped except those that match entries in the IP source guard binding table.

Packets received from interfaces or VLANs that do not have IP source guard enabled will not be checked by the IP source guard module and will be processed as normal.

Example

- Enable IP source guard on interface ge-1/1/3 and VLAN 20.

```
admin@PICOS# set ip-source-guard interface ge-1/1/3 vlan 20 enable true
admin@PICOS# commit
```

set ip-source-guard verify

The **set ip-source-guard verify** command configures IP source guard filtering item based on specific interface and VLAN.

The **delete ip-source-guard verify** command deletes the configuration.

Command Syntax

set ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify <ip | ip+mac>**

delete ip-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IP source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IP source guard static binding table, specifies the VLAN ID manually configured in IP source guard static binding table. • For IP source guard dynamic binding table, specifies the VLAN ID enabled DHCP snooping.
verify <ip | ip+mac>	Specifies the filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**. • When "**ip**" is specified, enables IP Source Guard with *interface* + *VLAN* + *Source IP* filtering. • When "**ip+mac**" is specified, enables IP Source Guard with *interface* + *VLAN* + *Source IP* + *Source MAC* address filtering. The default value is **ip**, IP Source Guard filtering item is interface + VLAN + Source IP.

Example

- Configure IP source guard filtering item based on specific interface and VLAN.

```
admin@PICOS# set ip-source-guard interface te-1/1/3 vlan 20 verify ip+mac
admin@PICOS# commit
```

set ip-source-guard traceoptions enable

The **set ip-source-guard traceoptions enable** command can be used to enable or disable debugging for tracing IP source guard operations.

The **delete ip-source-guard traceoptions enable** command deletes the configuration.

Command Syntax

set ip-source-guard traceoptions enable <**true** | **false**>

delete ip-source-guard traceoptions enable

Parameter

Parameter	Description
disable <**true** | **false**>	Enable or disable debugging for tracing IP source guard operations. The value could be **true** or **false**. • **true**: Disable debugging for tracing IP source guard operations. • **false**: Enable debugging for tracing IP source guard operations. By default, debugging for tracing IP source guard operations is disabled.

Example

- Enable debugging for tracing IP source guard operations.

```
admin@PICOS# set ip-source-guard traceoptions enable true
admin@PICOS# commit
```

run show ip-source-guard binding

The **run show ip-source-guard binding** command shows the IP source guard binding entries.

Command Syntax

run show ip-source-guard binding [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled IP source guard. The value could be a physical port.

Example

- View the IP source guard binding entries.

```
admin@PICOS# run show ip-source-guard binding
Total ipsg host count:     5
Mac-Address         Ip-Address      Interface       VLAN      Type         Filter-Type         Status
-------------------------------------------------------------------------------------------------------
22:22:22:22:22:22   1.1.1.1          ge-1/1/3        20        static        ip                  effective
33:33:33:33:33:33   1.1.1.1          te-1/1/3        20        static        ip                  ineffective
22:22:22:11:11:11   10.1.1.10        ge-1/1/3        4094      static        ip+mac              ineffective
22:22:22:11:11:20   20.1.1.10        ge-1/1/3        1         dhcp-snooping ip+mac              ineffective
22:22:22:22:22:22   20.20.20.22      ge-1/1/3        6         static        ip+mac              ineffective
```

In the show result,

- The parameter “**Type**” indicates the type of the entry, the value could be **static** or **dhcp-snooping**:
  - Ø **static**: indicates that the entry is manually configured.
  - Ø **dhcp-snooping**: indicates that the entry is originated from the DHCP snooping binding table.
- The parameter “**Filter-type**” indicates the IP source guard filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**,
  - Ø **ip**: enables IP Source Guard with *interface + VLAN + Source IP* filtering.
  - Ø **ip+mac**: enables IP Source Guard with *interface + VLAN + Source IP + Source MAC* address filtering.
- The parameter “**Status**” indicates whether the IP source guard binding entry is effective or not. After configuring the IP source guard binding entry, it needs to be deployed to the hardware by the system. If the entry is successfully deployed to the hardware, the "**Status**" will be shown as **effective**; however, if the deployment fails, it will be displayed as **ineffective**. Typically, the reason for deployment failure is due to the user configuring too many ACL rules, leading to insufficient hardware resources.

IPv6 Source Guard (IPSG for IPv6) Commands

- set ipv6-source-guard binding ip
- set ipv6-source-guard enable
- set ipv6-source-guard verify
- set ipv6-source-guard traceoptions enable
- run show ipv6-source-guard binding

set ipv6-source-guard binding ip

The **set ipv6-source-guard binding ip** command configures a static IPv6 source guard binding entry.

The **delete ipv6-source-guard binding ip** command deletes the configuration.

Command Syntax

set ipv6-source-guard binding ip <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*>

delete ipv6-source-guard binding ip<*ip_address*> [**mac** <*mac-address*> **interface**<*interface-name*>**vlan** <*vlan-id*>]

Parameter

Parameter	Description
ip <*ip_address*>	Specifies a source IPv6 address for the static binding entry. The IPv6 address should be an unicast address.
mac <*mac-address*>	Specifies a source MAC address for the static binding entry. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers, and cannot be all 0s, all Fs (a broadcast address), or a multicast address.
interface <*interface-name*>	Specifies ingress interface name for the static binding entry. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IPv6 source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

In IPv6 Source Guard, static binding entries involve manually associating IP addresses with specific interfaces on a network device. IPv6 Source Guard allows only traffic with matching source IP addresses and source MAC addresses to pass through the specified interface, thereby enhancing network security by preventing IP address spoofing attacks.

NOTE:

In the following example, a static IPv6 source guard binding entry is configured on the device. When attempting to delete this entry, an error occurs.

```
set ipv6-source-guard binding ip 100::6 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10

admin@PICOS# delete ipv6-source-guard binding ip 100::6 mac 00:00:00:00:00:01 interface ge-1/1/1 vlan 10
Deleting:
  10
OK
```

```
admin@PICOS# commit
IPSG6: vlan is required for ip 100::6, mac 00:00:00:00:00:01, interface ge-1/1/1
Commit failed.

admin@PICOS# delete ipv6-source-guard binding ip 100::6 mac 00:00:00:00:00:01
Deleting:
    00:00:00:00:00:01 {
                 interface "ge-1/1/1" {
                     vlan 10
        }
    }
OK
admin@PICOS# commit
IPSG6: mac is required for ip 100::6
Commit failed.
```

This is typically caused by the following two reasons:

- Due to the hierarchy structure design of PICOS CLI, when performing a deletion operation, the specified level and all its subordinate levels (i.e., the parameters and subsequent parameters in the command line) will be deleted, while the upper-level hierarchy (i.e., the parameters before the command line) will not be deleted.
- In the configuration of a static IPv6 source guard binding entry, the command **set ipv6-source-guard binding ip** <*ip_address*> **mac** <*mac-address*> **interface** <*interface-name*> **vlan** <*vlan-id*> requires all four parameters: IP address, MAC address, interface name, and VLAN ID, to be configured.

For this type of deletion error, you can complete the deletion configuration by removing the first hierarchy level **ipv6-source-guard binding ip**.

```
admin@PICOS# delete ipv6-source-guard binding ip 100::6
Deleting:
    100::6 {
        mac 00:00:00:00:00:01 {
            interface "ge-1/1/1" {
                vlan 10
            }
        }
    }
OK

admin@PICOS# commit
Commit OK.
Save done.
```

Example

- Configure a static IPv6 source guard binding entry manually.

```
admin@PICOS# set ipv6-source-guard binding ip 100::6 mac 22:22:22:11:11:11 interface ge-1/1/3 vlan 40
admin@PICOS# commit
```

set ipv6-source-guard enable

The **set ipv6-source-guard enable** command can be used to enable or disable IPv6 source guard function based on ingress interface and VLAN of the packet.

The **delete ipv6-source-guard enable** command deletes the configuration.

Command Syntax

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable** <**true | false**>

delete ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IPv6 source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IPv6 source guard static binding table, specifies the VLAN ID manually configured in IPv6 source guard static binding table. • For IPv6 source guard dynamic binding table, specifies the VLAN ID enabled DHCPv6 snooping.
enable <**true	false**>	Enable or disable IPv6 source guard function. The value could be **true** or **false**. • **true**: Enable IPv6 source guard function. • **false**: Disable IPv6 source guard function. By default, IPv6 source guard function is disabled.

Usage Guidelines

IPv6 source guard should be enabled based on specific interfaces and VLANs. When IPv6 source guard is enabled based on a specific interface and VLAN, all packets from that interface and VLAN will be dropped except those that match entries in the IPv6 source guard binding table.

Packets received from interfaces or VLANs that do not have IPv6 source guard enabled will not be checked by the IPv6 source guard module and will be processed as normal.

Example

- Enable IPv6 source guard on interface ge-1/1/3 and VLAN 20.

```
admin@PICOS# set ipv6-source-guard interface ge-1/1/3 vlan 20 enable true
admin@PICOS# commit
```

set ipv6-source-guard verify

The **set ipv6-source-guard verify** command configures IPv6 source guard filtering item based on specific interface and VLAN.

The **delete ipv6-source-guard verify** command deletes the configuration.

Command Syntax

set ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify <ip | ip+mac>**

delete ipv6-source-guard interface <*interface-name*> **vlan** <*vlan-id*> **verify**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an ingress interface name. The value is a physical port or a LAG port, such as ge-1/1/1, te-1/1/2, ae1. **Note**: IPv6 source guard be enabled on a physical interface or a Link Aggregation Group (LAG) interface but cannot be enabled on the member interfaces of a LAG.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094. • For IPv6 source guard static binding table, specifies the VLAN ID manually configured in IPv6 source guard static binding table. • For IPv6 source guard dynamic binding table, specifies the VLAN ID enabled DHCPv6 snooping.
verify <ip | ip+mac>	Specifies the filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**. • When "**ip**" is specified, enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* filtering. • When "**ip+mac**" is specified, enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* + *Source MAC* address filtering. The default value is **ip**, IPv6 Source Guard filtering item is interface + VLAN + Source IP.

Example

- Configure IPv6 source guard filtering item based on specific interface and VLAN.

```
admin@PICOS# set ipv6-source-guard interface te-1/1/3 vlan 20 verify ip+mac
admin@PICOS# commit
```

set ipv6-source-guard traceoptions enable

The **set ipv6-source-guard traceoptions enable** command can be used to enable or disable debugging for tracing IPv6 source guard operations.

The **delete ipv6-source-guard traceoptions enable** command deletes the configuration.

Command Syntax

set ipv6-source-guard traceoptions enable <**true** | **false**>

delete ipv6-source-guard traceoptions enable

Parameter

Parameter	Description
disable <**true** | **false**>	Enable or disable debugging for tracing IPv6 source guard operations. The value could be **true** or **false**. • **true**: Disable debugging for tracing IPv6 source guard operations. • **false**: Enable debugging for tracing IPv6 source guard operations. By default, debugging for tracing IPv6 source guard operations is disabled.

Example

- Enable debugging for tracing IPv6 source guard operations.

```
admin@PICOS# set ipv6-source-guard traceoptions enable true
admin@PICOS# commit
```

run show ipv6-source-guard binding

The **run show ipv6-source-guard binding** command shows the IPv6 source guard binding entries.

Command Syntax

run show ipv6-source-guard binding [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled IPv6 source guard. The value could be a physical port.

Example

- View the IPv6 source guard binding entries.

```
admin@PICOS# run show ipv6-source-guard binding
Total ipsg6 host count:     5
Mac-Address         Ip-Address      Interface       VLAN      Type         Filter-Type         Status
-------------------------------------------------------------------------------------------------------
22:22:22:22:22:22   2006::6           ge-1/1/3        20        static        ip                  effective
33:33:33:33:33:33   2007::7           te-1/1/3        20        static        ip                  ineffective
22:22:22:11:11:20   100::10           ge-1/1/3        1         dhcp6-snooping ip+mac              ineffective
22:22:22:22:22:22   2048::11          ge-1/1/3        6         static        ip+mac              ineffective
```

In the show result,

- The parameter “**Type**” indicates the type of the entry, the value could be **static** or **dhcp6-snooping**:
  - Ø **static**: indicates that the entry is manually configured.
  - Ø **dhcp6-snooping**: indicates that the entry is originated from the DHCPv6 snooping binding table.
- The parameter “**Filter-type**” indicates the IPv6 source guard filtering item based on specific interface and VLAN. The value could be **ip** or **ip+mac**,
  - Ø **ip**: enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* filtering.
  - Ø **ip+mac**: enables IPv6 Source Guard with *interface* + *VLAN* + *Source IP* + *Source MAC* address filtering.
- The parameter “**Status**” indicates whether the IPv6 source guard binding entry is effective or not. After configuring the IPv6 source guard binding entry, it needs to be deployed to the hardware by the system. If the entry is successfully deployed to the hardware, the "**Status**" will be shown as **effective**; however, if the deployment fails, it will be displayed as **ineffective**. Typically, the reason for deployment failure is due to the user configuring too many ACL rules, leading to insufficient hardware resources.

IS-IS commands

- set protocols isis area-tag network-entity
- set protocols isis area-tag is-type
- set protocols isis area-tag interface
- set protocols isis area-tag hostname-dynamic
- set protocols isis area-tag area-password authentication-type
- set protocols isis area-tag area-password authentication-key
- set protocols isis area-tag area-password authenticate-snp
- set protocols isis area-tag domain-password authentication-type
- set protocols isis area-tag domain-password authentication-key
- set protocols isis area-tag domain-password authenticate-snp
- set protocols isis area-tag attached-bit receive-ignore
- set protocols isis area-tag attached-bit send
- set protocols isis area-tag log-adjacency-changes
- set protocols isis area-tag metric-style
- set protocols isis area-tag set-overload-bit
- set protocols isis area-tag purge-originator
- set protocols isis area-tag lsp-mtu
- set protocols isis area-tag lsp-timers gen-interval
- set protocols isis area-tag lsp-timers refresh-interval
- set protocols isis area-tag lsp-timers max-lifetime
- set protocols isis area-tag spf-interval
- set protocols isis area-tag spf-delay-ietf init-delay
- set protocols isis area-tag spf-delay-ietf short-delay
- set protocols isis area-tag spf-delay-ietf long-delay
- set protocols isis area-tag spf-delay-ietf holddown
- set protocols isis area-tag spf-delay-ietf time-to-learn
- set protocols isis area-tag default-information originate
- set protocols isis area-tag default-information originate metric
- set protocols isis area-tag default-information originate route-map
- set protocols isis area-tag topology ipv6-unicast
- set protocols isis area-tag interface circuit-type
- set protocols isis area-tag interface csnp-interval
- set protocols isis area-tag interface psnp-interval
- set protocols isis area-tag interface hello-padding
- set protocols isis area-tag interface hello-interval
- set protocols isis area-tag interface hello-multiplier
- set protocols isis area-tag interface metric
- set protocols isis area-tag interface network point-to-point
- set protocols isis area-tag interface passive
- set protocols isis area-tag interface password authentication-type
- set protocols isis area-tag interface password authentication-key
- set protocols isis area-tag interface priority
- set protocols isis area-tag interface three-way-handshake
- set protocols isis area-tag interface bfd

- set protocols isis area-tag interface topology ipv6-unicast
- set protocols isis area-tag redistribute
- set protocols isis traceoption events
- set protocols isis traceoption adj-packets
- set protocols isis traceoption route-events
- set protocols isis traceoption snp-packets
- run show isis summary
- run show isis interface
- run show isis database
- run show isis hostname
- run show isis neighbor
- run show isis route
- run show isis topology

set protocols isis area-tag network-entity

The **set protocols isis area-tag network-entity** command configures network entity title (NET) provided in ISO format. The NET defines the current IS-IS area address and the system ID of the device.

The **delete protocols isis area-tag network-entity** command deletes the configuration.

NOTEs:

- The area address is used to uniquely identify different areas within a routing domain. All switches within the same Level-1 area must have the same area address, while switches within Level-2 areas can have different area addresses.
- Throughout the entire domain and backbone area, it is required to maintain a unique system ID.
- Currently, the switch supports only one IS-IS routing instance per VRF.
- Since a maximum of 3 area addresses can be configured in an IS-IS process, only up to 3 NETs can be configured.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **network-entity** <*network-entity*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **network-entity** <*network-entity*>

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
network-entity <*network-entity*>	Specifies the network entity title (NET) name.

Usage Guidelines

The NET consists of three parts:

- Area ID: The length of the Area ID can vary from 1 to 13 bytes.
- System ID: This part has a fixed length of 6 bytes.
- NSAP Selector (SEL): The last byte, different transport protocols correspond to different SELs. For IP, the SEL is always 00.

When configuring the NET parameter in IS-IS, ensure that these three components are properly defined according to your network requirements.

Example

- Define the NET as 32.0001.0040.0220.2030.00. The system ID is 0040.0220.2030 and the area ID is 32.0001.

```
admin@PICOS# set protocols isis area-tag instance1 network-entity 32.0001.0040.0220.2030.00
admin@PICOS# commit
```

set protocols isis area-tag is-type

The **set protocols isis area-tag is-type** command configures the level of the IS-IS switch.

The **delete protocols isis area-tag is-type** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **is-type**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
is-type <**level-1** | **level-1-2** | **level-2-only**>	Specifies the level of the IS-IS switch. The value could be **level-1**, **level-1-2** or **level-2-only**. The default value is **level-1-2**.

Example

- Configure the level of the IS-IS switch.

```
admin@PICOS# set protocols isis area-tag instance1 is-type level-1
admin@PICOS# commit
```

set protocols isis area-tag interface

The **set protocols isis area-tag interface** command enables IS-IS instance on a specific interface.

The **delete protocols isis area-tag interface** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> <**ipv4-routing | ipv6-routing**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> <**ipv4-routing | ipv6-routing**>

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface. By default, IS-IS is disabled on the interface.
<**ipv4-routing	ipv6-routing**>	Specifies the IP routing type.

Example

- Enable IS-IS instance on a specific interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 ipv4-routing
admin@PICOS# commit
```

set protocols isis area-tag hostname-dynamic

The **set protocols isis area-tag hostname-dynamic** command enables support for dynamic hostname.

The **delete protocols isis area-tag hostname-dynamic** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **hostname-dynamic** <**enable** | **disable**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **hostname-dynamic**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**enable** | **disable**>	Enable or disable dynamic hostname. The value could be **enable** or **disable**. • **enable**: Enable dynamic hostname. • **disable**: Disable dynamic hostname. By default, dynamic hostname is enabled.

Example

- Enable support for dynamic hostname.

```
admin@PICOS# set protocols isis area-tag instance1 hostname-dynamic enable
admin@PICOS# commit
```

set protocols isis area-tag area-password authentication-type

The **set protocols isis area-tag area-password authentication-type** command configures authentication type for the IS-IS area. The command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password authentication-key** <*password*> can be used to configure the authentication key. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag area-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authentication-type** <**simple | md5**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-type <**simple | md5**>	Specifies the authentication type. The value could be **simple** or **md5**. • **simple**: the password is specified as text in the authentication TLV. • **md5**: MD5 authentication provides much stronger authentication by computing the message digest (on the IS-IS PDU contents) using the secret key to produce a hashed message authentication code (HMAC). No default value.

Example

- Configure authentication type to *md5*.

```
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-key picos123456
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-type md5
admin@PICOS# commit
```

set protocols isis area-tag area-password authentication-key

The **set protocols isis area-tag area-password authentication-key** command configures authentication key for the IS-IS area. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag area-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **area-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authentication-key** <*password*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-key <*password*>	Specifies the authentication key. The value is a string, spaces and question mark are not allowed, case-sensitive, and can be 3 to 48 characters long.

Example

- Configure the authentication key.

```
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-key picos123456
admin@PICOS# set protocols isis area-tag instance1 area-password authentication-type md5
admin@PICOS# commit
```

set protocols isis area-tag area-password authenticate-snp

The **set protocols isis area-tag area-password authenticate-snp** command configures the authentication method for SNP messages in the IS-IS area. By default, IS-IS does not encapsulate authentication information for the sent SNP messages, nor perform authentication checks on the received SNP messages. Users can use this command to change this behavior.

The **delete protocols isis area-tag area-password authenticate-snp** command deletes the configuration.

> **NOTE:**
>
> Before configuring authenticate-snp, the authentication-type and authentication-key should be configured first.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authenticate-snp** <**none**|**send-only**|**validate**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **area-password authenticate-snp**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
none	IS-IS neither encapsulates authentication information for the sent SNP messages nor performs authentication checks on the received SNP messages.
send-only	Specifies encapsulating authentication information for generated LSPs and SNPs; only verify received LSPs, and do not verify received SNPs.
validate	IS-IS encapsulates authentication information for the sent SNP messages and performs authentication checks on the received SNP messages.

Example

- Configure the system only to encapsulate authentication information for the sent SNP messages for the IS-IS area.

```
admin@PICOS# set protocols isis area-tag instance1 area-password authenticate-snp send-only
admin@PICOS# commit
```

set protocols isis area-tag domain-password authentication-type

The **set protocols isis area-tag domain-password authentication-type** command configures authentication type for the IS-IS domain. The command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-key** <*password*> can be used to configure the authentication key. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag domain-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-type** <**simple | md5**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-type <**simple | md5**>	Specifies the authentication type. The value could be **simple** or **md5**. • **simple**: the password is specified as text in the authentication TLV. • **md5**: MD5 authentication provides much stronger authentication by computing the message digest (on the IS-IS PDU contents) using the secret key to produce a hashed message authentication code (HMAC). No default value.

Example

- Configure authentication type to *md5*.

```
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-type md5
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-key picos123456
admin@PICOS# commit
```

set protocols isis area-tag domain-password authentication-key

The **set protocols isis area-tag domain-password authentication-key** command configures authentication key for the IS-IS domain. IS-IS encapsulates authentication information for the sent IS-IS messages and performs authentication checks on the received messages.

The **delete protocols isis area-tag domain-password** command deletes the configuration.

- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **domain-password**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authentication-key** <*password*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
authentication-key <*password*>	Specifies the authentication key. The value is a string, spaces and question mark are not allowed, case-sensitive, and can be 3 to 48 characters long.

Example

- Configure the authentication key.

```
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-type md5
admin@PICOS# set protocols isis area-tag instance1 domain-password authentication-key picos123456
admin@PICOS# commit
```

set protocols isis area-tag domain-password authenticate-snp

The **set protocols isis area-tag domain-password authenticate-snp** command configures the authentication method for SNP messages for the IS-IS domain. By default, IS-IS does not encapsulate authentication information for the sent SNP messages, nor perform authentication checks on the received SNP messages. Users can use this command to change this behavior.

The **delete protocols isis area-tag domain-password authenticate-snp** command deletes the configuration.

> **NOTE:**
>
> Before configuring authenticate-snp, the authentication-type and authentication-key should be configured first.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authenticate-snp** <**send-only**|**validate**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **domain-password authenticate-snp**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
send-only	Specifies encapsulating authentication information for generated LSPs and SNPs; only verify received LSPs, and do not verify received SNPs.
validate	IS-IS encapsulates authentication information for the sent SNP messages and performs authentication checks on the received SNP messages.

Example

- Configure the system only to encapsulate authentication information for the sent SNP messages for the IS-IS domain.

```
admin@PICOS# set protocols isis area-tag instance1 domain-password authenticate-snp send-only
admin@PICOS# commit
```

set protocols isis area-tag attached-bit receive-ignore

The **set protocols isis area-tag attached-bit receive-ignore** command can be configured to prevent Level-1 routers from generating default routes due to the ATT bit. After configuration, Level-1 routers will not generate default routes in the routing table due to the ATT bit.

The **delete protocols isis area-tag attached-bit receive-ignore** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit receive-ignore** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit receive-ignore**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
receive-ignore <**true** | **false**>	Specifies whether Level-1 routers generate default routes due to the ATT bit. The value could be **true** or **false**. • **true**: Level-1 routers don't generate default routes due to the ATT bit. • **false**: Level-1 routers generate default routes due to the ATT bit. The default value is **false**.

Usage Guidelines

The ATT bit is a field in IS-IS LSP (Link State Packet) messages used to indicate whether a Level-1 area is connected to other areas. Level-1-2 routers set this field in their generated Level-1 LSPs to inform Level-1 routers within the same area that they are connected to other areas, specifically to the Level-2 backbone area. When routers in a Level-1 area receive Level-1 LSPs with the ATT bit set from Level-1-2 routers, they create a default route pointing to the Level-1-2 router as the destination, allowing data to be routed to other areas.

To prevent Level-1 routers from generating default routes due to the ATT bit, this command can be configured. After configuration, Level-1 routers will not send default routes in the routing table due to the ATT bit.

Example

- Configure Level-1 routers not to generate default routes in the routing table due to the ATT bit.

```
admin@PICOS# set protocols isis area-tag instance1 attached-bit receive-ignore true
admin@PICOS# commit
```

set protocols isis area-tag attached-bit send

The **set protocols isis area-tag attached-bit send** command configures that whether the Level-1-2 routers set ATT bit in the LSP sent to Level-1 routers.

The **delete protocols isis area-tag attached-bit send** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit send** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **attached-bit send**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
send <**true**	**false**>	Specifies whether the Level-1-2 routers set ATT bit in the LSP sent to Level-1 routers. The value could be **true** or **false**. • **true**: Level-1-2 routers set ATT bit in the LSP sent to Level-1 routers. • **false**: Level-1-2 routers don't set ATT bit in the LSP sent to Level-1 routers. The default value is **true**.

Example

- Configure the Level-1-2 routers to set ATT bit in the LSP sent to Level-1 routers.

```
admin@PICOS# set protocols isis area-tag instance1 attached-bit send true
admin@PICOS# commit
```

set protocols isis area-tag log-adjacency-changes

The **set protocols isis area-tag log-adjacency-changes** command opens the log of neighbor status changes.

The **delete protocols isis area-tag log-adjacency-changes** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **log-adjacency-changes**

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **log-adjacency-changes**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

When IS-IS detects a change in neighbor relationships, record the change in the system log.

Example

- Open the log of neighbor status changes.

```
admin@PICOS# set protocols isis area-tag instance1 log-adjacency-changes
admin@PICOS# commit
```

set protocols isis area-tag metric-style

The **set protocols isis area-tag metric-style** command configures the metric behavior transmitted by this router and the received metric behavior that will be used for processing the SPF calculation by this router.

The **delete protocols isis area-tag metric-style** command deletes the configuration.

- If you need to modify the IS-IS route metric type, please configure the **metric-style** when setting up the basic IS-IS functions. Otherwise, changing the metric type during network operation will cause the IS-IS process to restart, which may lead to neighbor disconnections.
- When setting the IS-IS metric type, be cautious as the metric type settings on the connected devices at both ends will affect link reachability.
- If the **metric-style** is not ***wide***, the metric value for IS-IS interface must be less than 64.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **metric-style** <**narrow** | **transition** | **wide**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **metric-style**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
metric-style <**narrow** | **transition** | **wide**>	Specifies the old-style (ISO 10589) or new-style packet formats. The value could be **narrow**, **transition** or **wide**. • **narrow**: transmit only narrow IS-IS metrics and to only process received narrow metrics from other routers for this router's SPF calculation. • **transition**: transmit both narrow and wide metrics, and if both metrics are received, to process the narrow metrics for this router's SPF calculation. If only wide metrics are received, wide metrics will be used for this router's SPF calculation. • **wide**: transmit only wide IS-IS metrics, and to only process received wide metrics from other routers for this router's SPF calculation. The default value is **wide**.

Usage Guidelines

Configuring metric style determines which metric behavior received from other IS-IS routers will be processed for this router's SPF calculation, and which metric behavior will be transmitted to other IS-IS routers by this router. The metric style used by an IS-IS router can be either narrow or wide.

Example

- Configure to transmit only narrow IS-IS metrics.

```
admin@PICOS# set protocols isis area-tag instance1 metric-style narrow
admin@PICOS# commit
```

set protocols isis area-tag set-overload-bit

The **set protocols isis area-tag set-overload-bit** command configures the overload bit for non-pseudonode LSPs.

The **delete protocols isis area-tag set-overload-bit** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **set-overload-bit** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **set-overload-bit**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**true** | **false**>	Specifies whether to configure the overload bit for non-pseudonode LSPs. The value could be **true** or **false**. • **true**: configure the overload bit for non-pseudonode LSPs. • **false**: not configure the overload bit for non-pseudonode LSPs. The default value is **false**.

Usage Guidelines

Although an LSP with the overload bit set will propagate throughout the network, it will not be used when calculating routes through an overloaded switch. That is to say, after setting the overload bit for a switch, other switches will not consider this switch when performing SPF calculations. However, direct routes to this switch will not be ignored.

Example

- Configure the overload bit for non-pseudonode LSPs.

```
admin@PICOS# set protocols isis area-tag instance1 set-overload-bit true
admin@PICOS# commit
```

set protocols isis area-tag purge-originator

The **set protocols isis area-tag purge-originator** command is used to enable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. Once this functionality is enabled, if dynamic hostname configuration is also set locally, the hostname TLV will be added in the PURGE messages as well.
The **delete protocols isis area-tag purge-originator** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **purge-originator** <**true** | **false**>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **purge-originator**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**true** | **false**>	Enable or disable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. The value could be **true** or **false**. • **true**: enable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. • **false**: disable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally. The default value is **false**.

Usage Guidelines

When the Remaining Lifetime field of an LSP message is 0, it indicates that the message has expired, and it is then referred to as a PURGE message. Typically, PURGE messages do not contain any information about the device that generated them, making it difficult to identify the source of the message when network issues occur.

To address this issue, the **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **purge-originator** command can be used to add the POI (Purge-Originator-Identification) TLV in PURGE messages sent by IS-IS devices. Additionally, if dynamic hostname configuration is enabled locally, the hostname TLV will also be added to the PURGE messages, providing convenience for troubleshooting purposes.

Example

- Enable the functionality of adding the Purge-Originator-Identification (POI) TLV in the PURGE messages sent by IS-IS locally.

```
admin@PICOS# set protocols isis area-tag instance1 purge-originator true
admin@PICOS# commit
```

set protocols isis area-tag lsp-mtu

The **set protocols isis area-tag lsp-mtu** command configures the maximum size of generated LSPs, in bytes.

The **delete protocols isis area-tag lsp-mtu** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-mtu** <*max-size*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-mtu**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
lsp-mtu <*max-size*>	Specifies the maximum size of generated LSPs. The value is an integer ranging from 128 to 4352 bytes. The default value is 1497 bytes.

Usage Guidelines

This command configures the size of the LSP (Link State Protocol) messages generated and received by the current IS-IS system.

NOTE:

Make sure that the length of the LSP is smaller than the MTU (Maximum Transmission Unit) of the IS-IS interface, otherwise, the LSP messages cannot be sent properly.

Example

- Configure the maximum size of generated LSPs.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-mtu 1024
admin@PICOS# commit
```

set protocols isis area-tag lsp-timers gen-interval

The **set protocols isis area-tag lsp-timers gen-interval** command configures the minimum interval in seconds between regenerating same LSP.
The **delete protocols isis area-tag lsp-timers** command deletes the configuration.

When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers**, and all the **lsp-timers** configuration of **gen-interval**, **refresh-interval** and **max-lifetime** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers gen-interval** <*lsp-gen-interval*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
gen-interval <*lsp-gen-interval*>	Specifies the minimum interval between regenerating same LSP. The value is an integer ranging from 1 to 120 seconds. The default value is 30 seconds.

Usage Guidelines

When there are changes in local routing information, the device needs to generate new LSPs to announce these changes. When changes in local routing information occur frequently, immediately generating new LSPs consumes a large amount of system resources. To speed up network convergence without affecting system performance, you can adjust the interval between LSP generations using this command.

Example

- Configure the minimum interval in seconds between regenerating same LSP.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-timers gen-interval 50
admin@PICOS# commit
```

set protocols isis area-tag lsp-timers refresh-interval

The **set protocols isis area-tag lsp-timers refresh-interval** command configures the refresh interval for LSPs.
The **delete protocols isis area-tag lsp-timers** command deletes the configuration.

- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers**, and all the **lsp-timers** configuration of **gen-interval**, **refresh-interval** and **max-lifetime** will be removed.
- The LSP maximum lifetime must exceed the refresh interval by more than 300.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers refresh-interval** <*lsp-refresh-interval*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
refresh-interval <*lsp-refresh-interval*>	Specifies the refresh interval for LSPs. The value is an integer ranging from 1 to 65235 seconds. The default value is 900 seconds.

Usage Guidelines

The flooding of LSPs (Link State Packets) requires periodic refreshing because when a device generates its system LSP, it includes the maximum valid time for the LSP. As other devices receive this LSP, its valid time decreases over time. If a device does not receive an updated LSP, once the valid time of the LSP reaches 0, it will be retained for an additional 60 seconds. If a new LSP is not received within this time, the LSP will be deleted.

By using command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers refresh-interval** <*lsp-refresh-interval*> to configure the refresh period for LSPs, it ensures that LSPs remain within their valid period and controls the convergence speed of the network.

Example

- Configure the refresh interval for LSPs.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-timers refresh-interval 1800
admin@PICOS# commit
```

set protocols isis area-tag lsp-timers max-lifetime

The **set protocols isis area-tag lsp-timers max-lifetime** command configures the maximum valid time for the LSPs generated by IS-IS. Adjust the maximum valid time for LSPs to ensure the validity of old LSPs until updated LSPs are received.
The **delete protocols isis area-tag lsp-timers** command deletes the configuration.

- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **lsp-timers**, and all the **lsp-timers** configuration of **gen-interval**, **refresh-interval** and **max-lifetime** will be removed.
- The LSP maximum lifetime must exceed the refresh interval by more than 300.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers max-lifetime** <*max-lsp-lifetime*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **lsp-timers**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
max-lifetime <*max-lsp-lifetime*>	Specifies the maximum valid time for the LSPs generated by IS-IS. The value is an integer ranging from 350 to 65535 seconds. The default value is 1200 seconds.

Usage Guidelines

The maximum lifetime of a link-state packet determines how long a link state packet will be propagated around the network before it is considered unusable. When an LSP's age reaches the 0, the packet is no longer usable.

Example

- Configure the maximum valid time for the LSPs generated by IS-IS.

```
admin@PICOS# set protocols isis area-tag instance1 lsp-timers max-lifetime 2000
admin@PICOS# commit
```

set protocols isis area-tag spf-interval

The **set protocols isis area-tag spf-interval** command configures the interval time for SPF (Shortest Path First) calculation.

The **delete protocols isis area-tag spf-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-interval** <*spf-interval*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
spf-interval <*spf-interval*>	Specifies the interval time for SPF (Shortest Path First) calculation. The value is an integer ranging from 1 to 120 seconds. The default value is 1 seconds.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

Example

- Configure the interval time for SPF (Shortest Path First) calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-interval 60
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf init-delay

The **set protocols isis area-tag spf-delay-ietf init-delay** command configures the initial delay in SPF calculation.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf init-delay** <*init-delay*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
init-delay <*init-delay*>	Specifies the initial delay in SPF calculation. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

To expedite route convergence speed without compromising the efficiency of switch modules, intelligent timers are utilized in SPF (Shortest Path First) calculations. These timers automatically adjust the delay time based on the frequency of changes in the Link State Database (LSDB).

Example

- Configure the initial delay in SPF calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf init-delay 50
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf short-delay

The **set protocols isis area-tag spf-delay-ietf short-delay** command configures the short delay in SPF calculation.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf short-delay** <*short-delay*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
short-delay <*short-delay*>	Specifies the short delay in SPF calculation. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

To expedite route convergence speed without compromising the efficiency of switch modules, intelligent timers are utilized in SPF (Shortest Path First) calculations. These timers automatically adjust the delay time based on the frequency of changes in the Link State Database (LSDB).

Example

- Configure the short delay in SPF calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf short-delay 10
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf long-delay

The **set protocols isis area-tag spf-delay-ietf long-delay** command configures the long delay in SPF calculation.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf long-delay** <*long-delay*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
long-delay <*long-delay*>	Specifies the long delay in SPF calculation. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

When there are changes in the Link State Database (LSDB), route calculations are necessary. However, frequent route calculations can consume a significant amount of system resources, leading to a decline in system performance. Delaying SPF (Shortest Path First) calculations can improve the efficiency of route calculations to some extent. On the other hand, if the delay in route calculations is too long, it may slow down the convergence speed of the routes.

To expedite route convergence speed without compromising the efficiency of switch modules, intelligent timers are utilized in SPF (Shortest Path First) calculations. These timers automatically adjust the delay time based on the frequency of changes in the Link State Database (LSDB).

Example

- Configure the long delay in SPF calculation.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf long-delay 500
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf holddown

The **set protocols isis area-tag spf-delay-ietf holddown** command configures the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times.

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf holddown** <*holddown*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
holddown <*holddown*>	Specifies the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Example

- Configure the time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf holddown 120
admin@PICOS# commit
```

set protocols isis area-tag spf-delay-ietf time-to-learn

The **set protocols isis area-tag spf-delay-ietf time-to-learn** command configure the maximum duration typically needed to learn all the IGP events related to a single component failure (such as router failure or SRLG failure).

The **delete protocols isis area-tag spf-delay-ietf** command deletes the configuration.

- When configuring, the **spf-delay-ietf** set of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**, and all the **spf-delay-ietf** configuration of **init-delay**, **short-delay**, **long-delay**, **holddown** and **time-to-learn** will be removed.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf time-to-learn** <*time-to-learn*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **spf-delay-ietf**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
time-to-learn <*time-to-learn*>	Specifies the maximum duration typically needed to learn all the IGP events related to a single component failure. The value is an integer ranging from 0 to 60000 milliseconds. No default value.

Usage Guidelines

It's mostly dependent on failure detection time variation between all routers that are adjacent to the failure. Additionally, it may depend on the different IGP implementations/parameters across the network and their relation to the origination and flooding of link state advertisements.

Example

- Configure the maximum duration typically needed to learn all the IGP events related to a single component failure.

```
admin@PICOS# set protocols isis area-tag instance1 spf-delay-ietf time-to-learn 3600
admin@PICOS# commit
```

set protocols isis area-tag default-information originate

The **set protocols isis area-tag default-information originate** command generates a default route in IS-IS route. Adding **always** argument to the "default-infomation orginate" statement essentially skips the checking for a default route already being installed in the table.

The **delete protocols isis area-tag default-information originate** command deletes the configuration.

When specifying the level of the IS-IS switch in this command, it should correspond with the **is-type** configuration in command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> [**always**]

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**><**level-1** | **level-2**> [**always**]

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing**	**ipv6-routing**>	Specifies the IP network type.
<**level-1**	**level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.

Example

- Generate a default route in IS-IS route.

```
admin@PICOS# set protocols isis area-tag instance1 default-information originate ipv4-routing level-1 always
admin@PICOS# commit
```

set protocols isis area-tag default-information originate metric

The **set protocols isis area-tag default-information originate metric** command configures the metric for the default route in IS-IS route.

The **delete protocols isis area-tag default-information originate metric** command deletes the configuration.

> When specifying the level of the IS-IS switch in this command, it should correspond with the **is-type** set in command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **metric** <*metric*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **metric**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing**	**ipv6-routing**>	Specifies the IP network type.
<**level-1**	**level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.
metric <*metric*>	Specifies the metric for the generated default route. The value is an integer ranging from 0 to 16777215.

Example

- Configure the metric for the default route in IS-IS route.

```
admin@PICOS# set protocols isis area-tag instance1 default-information originate ipv4-routing level-1 metric 50
admin@PICOS# commit
```

set protocols isis area-tag default-information originate route-map

The **set protocols isis area-tag default-information originate route-map** command configures the route map for the default route in IS-IS route.

The **delete protocols isis area-tag default-information originate route-map** command deletes the configuration.

When specifying the level of the IS-IS switch in this command, it should correspond with the **is-type** set in command **set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **is-type** <**level-1** | **level-1-2** | **level-2-only**>.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **route-map** <*route-map*>

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **default-information originate** <**ipv4-routing** | **ipv6-routing**> <**level-1** | **level-2**> **route-map**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing**	**ipv6-routing**>	Specifies the IP network type.
<**level-1**	**level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.
route-map <*route-map*>	Specifies the route map name for the generated default route. The value is a string.

Example

- Configure the route map for the default route in IS-IS route.

```
admin@PICOS# set protocols isis area-tag instance1 default-information originate ipv4-routing level-1 route-map map1
admin@PICOS# commit
```

set protocols isis area-tag topology ipv6-unicast

The **set protocols isis area-tag topology ipv6-unicast** command enables an IPv6 unicast topology for IS-IS.

The **delete protocols isis area-tag topology ipv6-unicast** command deletes the configuration.

To enable IPv6 unicast topology for IS-IS, the **metric-style** configuration should not be **narrow**.

Command Syntax

set protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **topology ipv6-unicast** [**overload**]

delete protocols isis area-tag <*text*> [**vrf** <*vrf-name*>] **topology ipv6-unicast**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example

- Enable an IPv6 unicast topology for IS-IS.

```
admin@PICOS# set protocols isis area-tag instance1 topology ipv6-unicast
admin@PICOS# commit
```

set protocols isis area-tag interface circuit-type

The **set protocols isis area-tag interface circuit-type** command configures circuit type for interface.

The **delete protocols isis area-tag interface circuit-type** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **circuit-type** <**level-1** | **level-1-2** | **level-2**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **circuit-type** <**level-1** | **level-1-2** | **level-2**>

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
circuit-type <**level-1**	**level-1-2**	**level-2**>	Specifies the circuit type for interface. • **level-1**: Level-1 only adjacencies are formed. • **level-1-2**: Level-1-2 adjacencies are formed. • **level-2**: Level-2 only adjacencies are formed.

Example

- Configure circuit type for interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 circuit-type level-1
admin@PICOS# commit
```

set protocols isis area-tag interface csnp-interval

The **set protocols isis area-tag interface csnp-interval** command is used to specify the interval for sending CSNP messages on a broadcast network.

The **delete protocols isis area-tag interface csnp-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **csnp-interval** <*csnp-interval*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **csnp-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
csnp-interval <*csnp-interval*>	Specifies the interval for sending CSNP messages. The value is an integer ranging from 1 to 600 seconds. The default value is 10 seconds.

Example

- Configure the interval for sending CSNP messages on a broadcast network.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 csnp-interval 50
admin@PICOS# commit
```

set protocols isis area-tag interface psnp-interval

The **set protocols isis area-tag interface psnp-interval** command configures the Partial Sequence Number Packets (PSNP) interval in seconds.

The **delete protocols isis area-tag interface psnp-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **psnp-interval** <*psnp-interval*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **psnp-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
psnp-interval <*psnp-interval*>	Specifies the Partial Sequence Number Packets (PSNP) interval. The value is an integer ranging from 1 to 120 seconds. The default value is 2 seconds.

Example

- Configure the Partial Sequence Number Packets (PSNP) interval.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 psnp-interval 50
admin@PICOS# commit
```

set protocols isis area-tag interface hello-padding

The **set protocols isis area-tag interface hello-padding** command is used to configure IS-IS interfaces to send standard Hello messages with padding fields.

The **delete protocols isis area-tag interface hello-padding** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-padding** <**enable** | **disable**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-padding**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
hello-padding <**enable** | **disable**>	Enable or disable IS-IS interfaces to send standard Hello messages with padding fields. The value could be **enable** or **disable**. • **enable**: Enables IS-IS interfaces to send standard Hello messages with padding fields. • **disable**: Disables IS-IS interfaces to send standard Hello messages with padding fields. By default, IS-IS interfaces send standard Hello messages with padding fields.

Example

- Configure IS-IS interfaces to send standard Hello messages with padding fields.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-padding enable
admin@PICOS# commit
```

set protocols isis area-tag interface hello-interval

The **set protocols isis area-tag interface hello-interval** command is used to specify the interval time for sending Hello messages on an IS-IS interface.

The **delete protocols isis area-tag interface hello-interval** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-interval** <*hello-interval*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-interval**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
hello-interval <*hello-interval*>	Specifies the interval for sending Hello messages. The value is an integer ranging from 1 to 600 seconds. The default value is 3 seconds.

Example

- Configure the interval time for sending Hello messages on an IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-interval 30
admin@PICOS# commit
```

set protocols isis area-tag interface hello-multiplier

The **set protocols isis area-tag interface hello-multiplier** command configures the multiplier for the interval time between Hello messages, in order to modify the neighbor hold time of IS-IS. The neighbor hold time is **hello-interval** x **hello-multiplier**.

The **delete protocols isis area-tag interface hello-multiplier** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-multiplier** <*integer*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **hello-multiplier**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
hello-multiplier <*integer*>	Specifies the neighbor hold time as a multiple of the interval time between Hello messages. The value is an integer ranging from 2 to 100. The default value is 10.

Example

- Configure the multiplier for the interval time between Hello messages.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 hello-multiplier 30
admin@PICOS# commit
```

set protocols isis area-tag interface metric

The **set protocols isis area-tag interface metric** command configures default metric value for IS-IS interface.

The **delete protocols isis area-tag interface metric** command deletes the configuration.

If the **metric-style** is not ***wide***, the metric value for IS-IS interface must be less than 64.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **metric** <*metric*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **metric**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
metric <*metric*>	Specifies the default metric value for IS-IS interface. The value is an integer ranging from 0 to 16777215. The default value is 10.

Example

- Configure the default metric value for IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 metric 100
admin@PICOS# commit
```

set protocols isis area-tag interface network point-to-point

The **set protocols isis area-tag interface network point-to-point** command configures network type to ‘Point-to-Point’ (broadcast by default) .

The **delete protocols isis area-tag interface network point-to-point** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **network point-to-point**

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **network point-to-point**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.

Example

- Configure network type to ‘Point-to-Point’.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 network point-to-point
admin@PICOS# commit
```

set protocols isis area-tag interface passive

The **set protocols isis area-tag interface passive** command configures the specified layer 3 interface as passive IS-IS interface.

The **delete protocols isis area-tag interface passive** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **passive**

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **passive**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.

Example

- Configure the specified layer 3 interface as passive IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 passive
admin@PICOS# commit
```

set protocols isis area-tag interface password authentication-type

The **set protocols isis area-tag interface password authentication-type** command configures authentication type for the IS-IS interface.

The **delete protocols isis area-tag interface password** command deletes the configuration.

- Make sure that the authentication configuration per interface on both ends of IS-IS neighbor is consistent, otherwise neighbors cannot be established.
- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> **interface** <*interface-name*> **password**.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **password authentication-type** <**simple | md5**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
authentication-type <**simple | md5**>	Specifies the authentication type. The value could be **simple** or **md5**. • **simple**: the password is specified as text in the authentication TLV. • **md5**: MD5 authentication provides much stronger authentication by computing the message digest (on the IS-IS PDU contents) using the secret key to produce a hashed message authentication code (HMAC). No default value.

Example

- Configure authentication type for the IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 password authentication-type md5
admin@PICOS# commit
```

set protocols isis area-tag interface password authentication-key

The **set protocols isis area-tag interface password authentication-key** command configures authentication password for the IS-IS interface.

The **delete protocols isis area-tag interface password** command deletes the configuration.

- Make sure that the authentication configuration per interface on both ends of IS-IS neighbor is consistent, otherwise neighbors cannot be established.
- When configuring, **authentication-type** and **authentication-key** should be submitted in the same commit.
- When deleting, the command is **delete protocols isis area-tag** <*text*> **interface** <*interface-name*> **password**.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **password authentication-key** <*password*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **password**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
authentication-key <*password*>	Specifies the authentication key. The value is a string, spaces and question mark are not allowed, case-sensitive, and can be 3 to 48 characters long.

Example

- Configure the authentication key.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 password authentication-key picos123456
admin@PICOS# commit
```

set protocols isis area-tag interface priority

The **set protocols isis area-tag interface priority** command configures priority for Designated Router election.

The **delete protocols isis area-tag interface priority** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **priority** <*priority*>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **priority**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
priority <*priority*>	Specifies the priority for Designated Router election. The value is an integer ranging from 0 to 127. The default value is 64. The higher the value, the higher the priority.

Example

- Configure the priority for Designated Router election.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 priority 85
admin@PICOS# commit
```

set protocols isis area-tag interface three-way-handshake

The **set protocols isis area-tag interface three-way-handshake** command is used to enable or disable the Three-Way Handshake for P2P adjacencies. Three-Way Handshake is enabled by default.
The **delete protocols isis area-tag interface three-way-handshake** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **three-way-handshake** <**enable** | **disable**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **three-way-handshake**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
three-way-handshake <**enable** | **disable**>	Enable or disable the Three-Way Handshake for P2P adjacencies. The value could be **enable** or **disable**. • **enable**: Enables the Three-Way Handshake for P2P adjacencies. • **disable**: Disables the Three-Way Handshake for P2P adjacencies. The default value is enable.

Example

- Disable the Three-Way Handshake for P2P adjacencies.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 three-way-handshake disable
admin@PICOS# commit
```

set protocols isis area-tag interface bfd

The **set protocols isis area-tag interface bfd** command configures parameters for Bidirectional Forwarding Detection (BFD) sessions on a specified IS-IS interface.

The **delete protocols isis area-tag interface bfd** command deletes the configuration.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **bfd** [**profile** <text>]

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **bfd**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
profile <text>	Optional. Specifies the BFD profile name. The value is a string.

Example

- Configure parameters for Bidirectional Forwarding Detection (BFD) sessions on a specified IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 bfd profile profile1
admin@PICOS# commit
```

set protocols isis area-tag interface topology ipv6-unicast

The **set protocols isis area-tag interface topology ipv6-unicast** command enables an IPv6 unicast topology on a specified IS-IS interface.

The **delete protocols isis area-tag interface topology ipv6-unicast** command deletes the configuration.

To enable an IPv6 unicast topology on a specified IS-IS interface, users have to enable the global configuration (**set protocols isis area-tag** <*text*> [**vrf** <*vrf-name*>] **topology ipv6-unicast** [**overload**]) first.

Command Syntax

set protocols isis area-tag <*text*> **interface** <*interface-name*> **topology ipv6-unicast** <**enable** | **disable**>

delete protocols isis area-tag <*text*> **interface** <*interface-name*> **topology ipv6-unicast**

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
interface <*interface-name*>	Specifies an L3 interface to enable IS-IS. The value could be a VLAN interface, routed interface or sub-interface.
<**enable** | **disable**>	Enables or disables an IPv6 unicast topology on a specified IS-IS interface. The value could be **enable** or **disable**. • **enable**: Enables an IPv6 unicast topology on a specified IS-IS interface. • **disable**: Disables an IPv6 unicast topology on a specified IS-IS interface. The default value is enable.

Example

- Enable an IPv6 unicast topology on a specified IS-IS interface.

```
admin@PICOS# set protocols isis area-tag instance1 interface vlan10 topology ipv6-unicast enable
admin@PICOS# commit
```

set protocols isis area-tag redistribute

The command **set protocols isis area-tag redistribute** redistributes routes of a specified type or protocol into IS-IS.

The command **delete protocols isis area-tag redistribute** removes this configuration.

Command Syntax

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2> [metric** <*metric*>**]**

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute** <**ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2> [metric** <*metric*>**]**

set protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2> metric**

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute** <**ipv4-routing {bgp|connected|kernel|static|ospf|rip|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2> metric**

delete protocols isis area-tag <*text*> **[vrf** <*vrf-name*>**] redistribute ipv6-routing {bgp|connected|kernel|static|ripng|ospf6|table** <*table-id*>**} <level-1 | level-2>** [**route-map** <*route-map*>]

Parameter

Parameter	Description
area-tag <*text*>	Specifies the IS-IS routing instance name. The value is a string.
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
<**ipv4-routing** | **ipv6-routing**>	Specifies the IP network type.
<**level-1** | **level-2**>	Specifies the level of the IS-IS switch. The value could be **level-1** or **level-2**.
bgp	Specifies the BGP routes for redistribution.
connected	Specifies the directly connected routes for redistribution.
kernel	Specifies the kernel routes for redistribution.
static	Specifies the static routes for redistribution.
ospf	Specifies the OSPF routes for redistribution.
ospf6	Specifies the OSPFv3 routes for redistribution.
rip	Specifies the RIP routes for redistribution.
ripng	Specifies the RIPng routes for redistribution.
table <*table-id*>	Specify a table for route redistribution. The value is an integer that ranges from 0 to 65535.
metric <*metric*>	Optional. Specifies the route metric. The value is an integer that ranges from 0 to 16777215.
route-map <*route-map*>	Optional. Specifies the route map name for the route. The value is a string.

Example

- Configure IS-IS to redistribute BGP routes into IS-IS with metric 5.

```
admin@PICOS# set protocols isis area-tag instance1 redistribute ipv4-routing bgp level-1 metric 5
admin@PICOS# commit
```

set protocols isis traceoption events

The **set protocols isis traceoption events** command can be used to enable or disable IS-IS debugging for event tracing.

The **delete protocols isis traceoption events** command deletes the configuration.

Command Syntax

set protocols isis traceoption events

delete protocols isis traceoption events

Parameters

Null.

Example

- Enable IS-IS debugging for event tracing.

```
admin@PICOS# set protocols isis traceoption events
admin@PICOS# commit
```

set protocols isis traceoption adj-packets

The **set protocols isis traceoption adj-packets** command can be used to enable or disable IS-IS debugging for IS-IS Adjacency related packets.

The **delete protocols isis traceoption adj-packets** command deletes the configuration.

Command Syntax

set protocols isis traceoption adj-packets

delete protocols isis traceoption adj-packets

Parameters

Null.

Example

- Enable IS-IS debugging for IS-IS Adjacency related packets.

```
admin@PICOS# set protocols isis traceoption adj-packets
admin@PICOS# commit
```

set protocols isis traceoption route-events

The **set protocols isis traceoption route-events** command can be used to enable or disable IS-IS debugging for IS-IS Route related events.

The **delete protocols isis traceoption route-events** command deletes the configuration.

Command Syntax

set protocols isis traceoption route-events

delete protocols isis traceoption route-events

Parameters

Null.

Example

- Enable IS-IS debugging for IS-IS Route related events.

```
admin@PICOS# set protocols isis traceoption route-events
admin@PICOS# commit
```

set protocols isis traceoption snp-packets

The **set protocols isis traceoption snp-packets** command can be used to enable or disable IS-IS debugging for IS-IS CSNP/PSNP packets.
The **delete protocols isis traceoption snp-packets** command deletes the configuration.

Command Syntax

set protocols isis traceoption snp-packets
delete protocols isis traceoption snp-packets

Parameters

Null.

Example

- Enable IS-IS debugging for IS-IS CSNP/PSNP packets.

```
admin@PICOS# set protocols isis traceoption snp-packets
admin@PICOS# commit
```

run show isis summary

The **run show isis summary** command shows summary information about IS-IS.

Command Syntax

run show isis [**vrf** <*text*>**| vrf all**] **summary** [**json**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.

Example

- View the summary information of the IS-IS configuration.

```
admin@PICOS# run show isis summary
vrf             : default
Process Id      : 977
System Id       : 0000.0000.0004
Up time         : 00:31:32 ago
Number of areas : 2
Area instance1:
  Net: 34.0000.0000.0004.00
  TX counters per PDU type:
   LSP RXMT: 0
  RX counters per PDU type:
  Level-1:
    LSP0 regenerated: 7
         LSPs purged: 0
    SPF:
      minimum interval  : 44
    IPv4 route computation:
      last run elapsed  : 00:11:40 ago
      last run duration : 47 usec
      run count         : 6
  Level-2:
    LSP0 regenerated: 7
         LSPs purged: 0
    SPF:
      minimum interval  : 44
    IPv4 route computation:
      last run elapsed  : 00:11:40 ago
      last run duration : 21 usec
      run count         : 6
```

run show isis interface

The **run show isis interface** command displays information about layer 3 interfaces participating in IS-IS process.

Command Syntax

run show isis [vrf <*text*> **| vrf all] interface** <*text*> [**detail**] [**json**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.
interface <*text*>	Specifies an interface name.

Example

- View information about layer 3 interfaces participating in IS-IS process.

```
admin@PICOS# run show isis interface vlan100
Area 1:
  Interface: vlan100, State: Up, Active, Circuit Id: 0x4c
    Type: lan, Level: L1L2, SNPA: 1c72.1dc9.1be1
    Level-1 Information:
      Metric: 10, Active neighbors: 1
      Hello interval: 3, Holddown count: 10 (pad)
      CNSP interval: 10, PSNP interval: 2
      LAN Priority: 64, is not DIS
    Level-2 Information:
      Metric: 10, Active neighbors: 1
      Hello interval: 3, Holddown count: 10 (pad)
      CNSP interval: 10, PSNP interval: 2
      LAN Priority: 64, is not DIS
    IP Prefix(es):
      1.1.1.1/24
    IPv6 Link-Locals:
      fe80::1e72:1d08:3c9:1be1/64
    IPv6 Prefixes:
      1000::1/64


admin@PICOS# run show isis interface
Area instance1:
  Interface   CircId   State    Type     Level
  vlan25      0x0      Config   p2p      L2
Area 1:
  Interface   CircId   State    Type     Level
  vlan10      0x4a     Up       lan      L1L2
  vlan100     0x4c     Up       lan      L1L2
  vlan200     0x4d     Up       lan      L1L2
```

run show isis database

The **run show isis database** command displays the Link State Database (LSDB) information of IS-IS.

Command Syntax

run show isis [vrf <*text*> **| vrf all] database** [**detail**] [**json**] [**lsp-id** <*lsp-id*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.
lsp-id <*lsp-id*>	Optional. Specifies the LSP ID to be displayed. The value is in the format of xxxx.xxxx.xxxx.xx-xx. For example, 0460.0600.6004.00-00.

Example

- View the Link State Database (LSDB) information of IS-IS.

```
admin@PICOS# run show isis database
Area 1:
IS-IS Level-1 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xc721     542    1/0/0
PICOS.00-00               143   0x00000008  0x7627     699    1/0/0
PICOS.b1-00                51   0x00000003  0xe79f     728    1/0/0
PICOS.00-00               106   0x00000005  0xc718     394    1/0/0
PICOS.b3-00                51   0x00000004  0xba45     367    1/0/0
    5 LSPs

IS-IS Level-2 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xbf31     561    0/0/0
PICOS.00-00               143   0x00000008  0x6e37     719    0/0/0
PICOS.b1-00                51   0x00000003  0xdfaf     712    0/0/0
PICOS.00-00               106   0x00000005  0xbf28     450    0/0/0
PICOS.b3-00                51   0x00000004  0xb255     380    0/0/0
    5 LSPs



admin@PICOS# run show isis database detail
Area 1:
IS-IS Level-1 link-state database:
LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xc721     508    1/0/0
  Protocols Supported: IPv4, IPv6
  Area Address: 49.0001
  Hostname: localhost
  TE Router ID: 10.10.51.179
  Router Capability: 10.10.51.179 , D:0, S:0
  Extended Reachability: 0000.0000.2222.b1 (Metric: 10)
  IPv4 Interface Address: 10.10.51.179
  Extended IP Reachability: 1.1.1.0/24 (Metric: 10)
  Extended IP Reachability: 10.10.10.0/24 (Metric: 10)
  IPv6 Reachability: 1000::/64 (Metric: 10)

PICOS.00-00               143   0x00000008  0x7627     665    1/0/0
  Protocols Supported: IPv4, IPv6
```

```
  Area Address: 49.0001
  Hostname: PICOS
  TE Router ID: 10.10.51.53
  Router Capability: 10.10.51.53 , D:0, S:0
  Extended Reachability: 0000.0000.2222.b1 (Metric: 10)
  Extended Reachability: 0000.0000.3333.b3 (Metric: 10)
  IPv4 Interface Address: 10.10.51.53
  Extended IP Reachability: 1.1.1.0/24 (Metric: 10)
  Extended IP Reachability: 2.2.2.0/24 (Metric: 10)
  IPv6 Reachability: 1000::/96 (Metric: 10)
  IPv6 Reachability: 2000::/96 (Metric: 10)

PICOS.b1-00               51   0x00000003  0xe79f     694    1/0/0
  Extended Reachability: 0000.0000.2222.00 (Metric: 0)
  Extended Reachability: 0000.0000.0004.00 (Metric: 0)

PICOS.00-00              106   0x00000005  0xc718     360    1/0/0
  Protocols Supported: IPv4, IPv6
  Area Address: 49.0001
  Hostname: PICOS
  TE Router ID: 10.10.51.171
  Router Capability: 10.10.51.171 , D:0, S:0
  Extended Reachability: 0000.0000.3333.b3 (Metric: 10)
  IPv4 Interface Address: 10.10.51.171
  Extended IP Reachability: 2.2.2.0/24 (Metric: 10)
  IPv6 Reachability: 2000::/96 (Metric: 10)

PICOS.b3-00               51   0x00000004  0xba45     333    1/0/0
  Extended Reachability: 0000.0000.3333.00 (Metric: 0)
  Extended Reachability: 0000.0000.2222.00 (Metric: 0)

    5 LSPs

IS-IS Level-2 link-state database:
LSP ID                 PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL
localhost.00-00      *    114   0x00000008  0xbf31     527    0/0/0
  Protocols Supported: IPv4, IPv6
  Area Address: 49.0001
  Hostname: localhost
  TE Router ID: 10.10.51.179
  Router Capability: 10.10.51.179 , D:0, S:0
  Extended Reachability: 0000.0000.2222.b1 (Metric: 10)
  IPv4 Interface Address: 10.10.51.179
  Extended IP Reachability: 1.1.1.0/24 (Metric: 10)
  Extended IP Reachability: 10.10.10.0/24 (Metric: 10)
  IPv6 Reachability: 1000::/64 (Metric: 10)
......
```

run show isis hostname

The **run show isis interface** command displays IS-IS hostname information.

Command Syntax

run show isis [vrf <*text*> **| vrf all] hostname**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.

Example

- View IS-IS hostname information.

```
admin@PICOS# run show isis hostname
vrf     : default
Level  System ID      Dynamic Hostname
2      0000.0000.2222 PICOS
2      0000.0000.3333 PICOS
     * 0000.0000.0004 localhost
```

run show isis neighbor

The **run show isis neighbor** command displays IS-IS neighbor information.

Command Syntax

run show isis [vrf <*text*> **| vrf all**] **neighbor** [**a-neighbor**<*text*>][**detail**] [**json**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.
a-neighbor<*text*>	Specifies the system ID of an IS-IS neighbor.

Example

- View IS-IS neighbor information.

```
admin@PICOS# run show isis neighbor
Area 1:
  System Id           Interface   L  State        Holdtime SNPA
  PICOS               vlan100     1  Up            27       8cea.1b4b.7821
  PICOS               vlan100     2  Up            28       8cea.1b4b.7821



admin@PICOS# run show isis neighbor a-neighbor PICOS
Area 1:
 PICOS
    Interface: vlan100, Level: 1, State: Up, Expires in 28s
    Adjacency flaps: 1, Last: 3m34s ago
    Circuit type: L1L2, Speaks: IPv4, IPv6
    SNPA: 8cea.1b4b.7821, LAN id: PICOS.b1
    LAN Priority: 64, is DIS, DIS flaps: 1, Last: 3m34s ago
    Area Address(es):
      49.0001
    IPv4 Address(es):
      1.1.1.2
    IPv6 Address(es):
      fe80::8eea:1b10:14b:7821
    Global IPv6 Address(es):
      1000::2

 PICOS
    Interface: vlan100, Level: 2, State: Up, Expires in 29s
    Adjacency flaps: 1, Last: 3m35s ago
    Circuit type: L1L2, Speaks: IPv4, IPv6
    SNPA: 8cea.1b4b.7821, LAN id: PICOS.b1
    LAN Priority: 64, is DIS, DIS flaps: 1, Last: 3m35s ago
    Area Address(es):
      49.0001
    IPv4 Address(es):
      1.1.1.2
    IPv6 Address(es):
      fe80::8eea:1b10:14b:7821
    Global IPv6 Address(es):
      1000::2
```

run show isis route

The **run show isis route** command shows route information about IS-IS.

Command Syntax

run show isis [vrf <*text*>**| vrf all]route** [**level-1**|**level-2**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.
[**level-1**|**level-2**]	Optional. Specifies the routing information for the type of router to be displayed.

Example

- View the route information of IS-IS.

```
admin@PICOS# run show isis route level-1
Area 1:
IS-IS L1 IPv4 routing table:

 Prefix      Metric  Interface  Nexthop  Label(s)
 -----------------------------------------------
 1.1.1.0/24  20      vlan100    1.1.1.2  -
 2.2.2.0/24  20      vlan100    1.1.1.2  -

IS-IS L1 IPv6 routing table:

 Prefix     Metric  Interface  Nexthop                  Label(s)
 ------------------------------------------------------------------
 1000::/64  0       -          -                        -
 1000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
 2000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -


admin@PICOS# run show isis route
Area 1:
IS-IS L1 IPv4 routing table:

 Prefix         Metric  Interface  Nexthop  Label(s)
 -------------------------------------------------
 1.1.1.0/24     20      vlan100    1.1.1.2  -
 2.2.2.0/24     20      vlan100    1.1.1.2  -
 10.10.10.0/24  0       -          -        -

IS-IS L1 IPv6 routing table:

 Prefix     Metric  Interface  Nexthop                  Label(s)
 ------------------------------------------------------------------
 1000::/64  0       -          -                        -
 1000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
 2000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -

IS-IS L2 IPv4 routing table:

 Prefix         Metric  Interface  Nexthop  Label(s)
 -------------------------------------------------
 1.1.1.0/24     20      vlan100    1.1.1.2  -
 2.2.2.0/24     20      vlan100    1.1.1.2  -
```

```
 10.10.10.0/24  0       -          -        -

IS-IS L2 IPv6 routing table:

 Prefix     Metric  Interface  Nexthop                   Label(s)
 ------------------------------------------------------------------
 1000::/64  0       -          -                         -
 1000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
 2000::/96  20      vlan100    fe80::8eea:1b10:14b:7821  -
```

run show isis topology

The **run show isis topology** command shows topology IS-IS paths to Intermediate Systems, globally, in area (level-1) or domain (level-2).

Command Syntax

run show isis [vrf <*text*>**| vrf all**] **topology** [**level-1**|**level-2**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name.
[**level-1**|**level-2**]	Optional. Specifies the topology IS-IS paths to Intermediate Systems, globally, in area (level-1) or domain (level-2).

Example

- View the topology IS-IS paths to Intermediate Systems, globally, in area (level-1) or domain (level-2).

```
admin@PICOS# run show isis topology level-1
Area 1:
IS-IS paths to level-1 routers that speak IP
Vertex               Type         Metric Next-Hop             Interface Parent
localhost
1.1.1.0/24           IP internal  0                                     localhost(4)
10.10.10.0/24        IP internal  0                                     localhost(4)
PICOS                TE-IS        10     PICOS                vlan100   localhost(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                TE-IS        20     PICOS                vlan100   PICOS(2)
1.1.1.0/24           IP TE        20     PICOS                vlan100   PICOS(4)
2.2.2.0/24           IP TE        20     PICOS                vlan100   PICOS(4)

IS-IS paths to level-1 routers that speak IPv6
Vertex               Type         Metric Next-Hop             Interface Parent
localhost
1000::/64            IP6 internal 0                                     localhost(4)
PICOS                TE-IS        10     PICOS                vlan100   localhost(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                TE-IS        20     PICOS                vlan100   PICOS(2)
1000::/96            IP6 internal 20     PICOS                vlan100   PICOS(4)
2000::/96            IP6 internal 20     PICOS                vlan100   PICOS(4)


admin@PICOS# run show isis topology level-2
Area 1:
IS-IS paths to level-2 routers that speak IP
Vertex               Type         Metric Next-Hop             Interface Parent
localhost
1.1.1.0/24           IP internal  0                                     localhost(4)
10.10.10.0/24        IP internal  0                                     localhost(4)
PICOS                TE-IS        10     PICOS                vlan100   localhost(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                pseudo_TE-IS 20     PICOS                vlan100   PICOS(4)
PICOS                TE-IS        20     PICOS                vlan100   PICOS(2)
1.1.1.0/24           IP TE        20     PICOS                vlan100   PICOS(4)
2.2.2.0/24           IP TE        20     PICOS                vlan100   PICOS(4)

IS-IS paths to level-2 routers that speak IPv6
Vertex               Type         Metric Next-Hop             Interface Parent
```

```
localhost
1000::/64           IP6 internal 0                                  localhost(4)
PICOS               TE-IS        10     PICOS              vlan100   localhost(4)
PICOS               pseudo_TE-IS 20     PICOS              vlan100   PICOS(4)
PICOS               pseudo_TE-IS 20     PICOS              vlan100   PICOS(4)
PICOS               TE-IS        20     PICOS              vlan100   PICOS(2)
1000::/96           IP6 internal 20     PICOS              vlan100   PICOS(4)
2000::/96           IP6 internal 20     PICOS              vlan100   PICOS(4)
```

ACL Configuration Commands

This section contains descriptions of the ACL commands that this chapter references.

- set firewall filter description
- set firewall filter input interface
- set firewall filter input vlan-interface
- set firewall filter input routed-interface
- set firewall filter output interface
- set firewall filter output vlan-interface
- set firewall filter output routed-interface
- set firewall filter sequence description
- set firewall filter sequence from destination-address-ipv4
- set firewall filter sequence from destination-address-ipv6
- set firewall filter sequence from destination-mac-address
- set firewall filter sequence from destination-port
- set firewall filter sequence from ether-type
- set firewall filter sequence from ip trust-mode
- set firewall filter sequence from ip value
- set firewall filter sequence from protocol icmp
- set firewall filter sequence from protocol igmp
- set firewall filter sequence from protocol ip
- set firewall filter sequence from protocol ospf
- set firewall filter sequence from protocol others
- set firewall filter sequence from protocol tcp
- set firewall filter sequence from protocol tcp flags
- set firewall filter sequence from protocol udp
- set firewall filter sequence from source-address-ipv4
- set firewall filter sequence from source-address-ipv6
- set firewall filter sequence from source-mac-address
- set firewall filter sequence from source-port
- set firewall filter sequence from vlan
- set firewall filter sequence then action
- set firewall filter sequence then forwarding-class
- set firewall filter sequence log interval
- set firewall system-output disable
- set firewall time-range periodic start
- set firewall time-range periodic end
- run show filter
- run show timerange

set firewall filter description

To configure the filter description, use the **set firewall filter description** command in L2/L3 configuration mode. To remove the filter desctiption, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **description** *filter-description*

delete firewall filter *fileter-name* **description**

Parameters

filter-name	Filter name.
filter-description	Filter description.

Example

The following example configures the filter named *MyFilter* with the description *It's a test filter*.

```
admin@Switch# set firewall filter MyFilter description "It's a test filter"
```

The folowing example removes the description of the filter *MyFilter*. Note that only the description is removed. The filter itself is not deleted by this command.

```
admin@Switch# delete firewall filter MyFilter description
Deleting:
>   description: "\"It's a test filter\""
OK
```

set firewall filter input interface

The **set firewall filter input interface** command applies firewall filter to the incoming packets at an interface. To remove the input interface from the filter, use the **delete** format of the command.

Command Syntax

set firewall filter <*filer-name*> **input interface** <*interface-name*>
delete firewall filter <*filer-name*> **input interface** <*interface-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Specifies filter name, the value is a string type, spaces are not allowed.
interface <*interface-name*>	Specifies a switch interface. The value could be a physical interface, a logic interface or **inbound-control-plane**. For example, te-1/1/49, ae1. **Note:** When the interface name is configured to **inbound-control-plane**, it means applying firewall filter to the incoming packets directed to switch CPU. As this function is substituted by CoPP feature, the value **inbound-control-plane** will have no effect. For details of CoPP, please refer to CoPP Configuration Guide.

Example

- Set the firewall filter f1 at interface te-1/1/49.

```
admin@Switch# set firewall filter f1 input interface te-1/1/49
```

set firewall filter input vlan-interface

To apply the filter to ingress packets on a VLAN interface, use the **set firewall filter input vlan-interface** command in L2/L3 configuration mode. To remove the filter from ingress packets on a VLAN interface, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **input vlan-interface** *vlan-interface-name*
delete firewall filter *filter-name* **input vlan-interface** *vlan-interface-name*

Parameters

filter-name	Filter name.
vlan-interface-name	VLAN interface name.

Example

The following example applies the *MyFilter* filter to ingress packets at the *vlan2* interface:

```
admin@Switch# set firewall filter MyFilter input vlan-interface vlan2
```

The following example removes the *MyFilter* filter from ingress packets at the *vlan2* interface:

```
admin@Switch# delete firewall filter MyFilter input vlan-interface vlan2
Deleting:
>   vlan2
OK
```

set firewall filter input routed-interface

To apply the filter to ingress packets on a routed interface, use the **set firewall filter input routed-interface** command in L2/L3 configuration mode. To remove the filter from ingress packets on a routed interface, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **input routed-interface** *routed-interface-name*
delete firewall filter *filter-name* **input routed-interface** *routed-interface-name*

Parameters

filter-name	Filter name.
routed-interface-name	Routed interface name.

Example

The following example applies the *MyFilter* filter to ingress packets at the *rif-ge3* interface:

```
admin@Switch# set firewall filter MyFilter input routed-interface rif-ge3
```

The following example removes the *MyFilter* filter from ingress packets at the rif-ge3 interface:

```
admin@Switch# delete firewall filter MyFilter input routed-interface rif-ge3
Deleting:
>   ge3
OK
```

set firewall filter output interface

To apply a filter to egress packets at an interface, use the **set firewall filter output interface** command in L2/L3 configuration mode. To remove the filter from an egress interface, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **output interface** *interface-name*
delete firewall filter *filter-name* **output interface** *interface-name*

Parameters

filter-name	Filter name.
interface-name	Interface name.

Example

The following example applies the *MyFilter* filter to egress packets on the *ge-1/1/2* interface:

```
admin@Switch# set firewall filter MyFiler output interface ge-1/1/2
```

The following example removes the *MyFilter* filter from egress packets on the *ge-1/1/2* interface:

```
admin@Switch# delete firewall filter MyFiler output interface ge-1/1/2
Deleting:
>   ge-1/1/2
OK
```

set firewall filter output vlan-interface

To apply a filter to egress packets at a VLAN interface, use the **set firewall filter output vlan-interface** command in L2/L3 configuration mode. To remove the filter, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **output vlan-interface** *vlan-interface-name*
delete firewall filter *filter-name* **output vlan-interface** *vlan-interface-name*

Parameters

filter-name	Filter name.
vlan-interface-name	VLAN interface name.

Example

This example applies the *MyFilter* filter to egress packets at the VLAN interface *vlan2*:

```
admin@Switch# set firewall filter MyFilter output vlan-interface vlan2
```

This example removes the *MyFilter* filter from egress packets at the VLAN interface *vlan2*:

```
admin@Switch# delete firewall filter MyFilter output vlan-interface vlan2
Deleting:
>   vlan2
OK
```

set firewall filter output routed-interface

To apply a filter to egress packets at a routed interface, use the **set firewall filter output routed-interface** command in L2/L3 configuration mode. To remove the filter, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **output routed-interface** *routed-interface-name*
delete firewall filter *filter-name* **output routed-interface** *routed-interface-name*

Parameters

filter-name	Filter name.
routed-interface-name	Routed interface name.

Example

This example applies the *MyFilter* filter to egress packets at the routed interface *rif-ge3*:

```
admin@Switch# set firewall filter MyFilter output routed-interface rif-ge3
```

This example removes the *MyFilter* filter from egress packets at the routed interface *rif-ge3*:

```
admin@Switch# delete firewall filter MyFilter output routed-interface rif-ge3
Deleting:
>   ge3
OK
```

set firewall filter sequence description

To configure the filter sequence description, use the **set firewall filter sequence description** command in L2/L3 configuration mode. To remove the filter sequence description, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** sequence-*number* **description** *sequence-description*
delete firewall filter *filter-name* **sequence** *number* **description**

Parameters

filter-name	Filter name.
sequence-number	The sequence number, smaller values representing higher priorities. The range is 0-9999.
sequence-description	The sequence description.

Example

The following example configures the description for sequence 10 of the *MyFilter* filter:

```
admin@Switch# set firewall filter MyFilter sequence 10 description "My filter sequence"
```

The following example removes the description for sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 description
Deleting:
>   description: "My filter sequence"
OK
```

set firewall filter sequence from destination-address-ipv4

To filter packets with a specific destination IP address, use the **set firewall filter sequence from destination-address-ipv4** command in L2/L3 configuration mode. To remove the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *sequence-number* **from destination-address-ipv4** *address/mask*
delete firewall filter *filter-name* **sequence** *sequence-number* **from destination-address-ipv4**

Parameters

filter-name	Filter name.
sequence-number	Filter sequence number. The range is 0-9999.
address/mask	IPv4 subnet and subnet mask. For example, 10.1.1.0/24.

Example

The following example configures sequence 1 of the *MyFilter* filter to drop packets to the destination IP address 192.168.1.1:

```
admin@Switch# set firewall filter MyFilter sequence 1 from destination-address-ipv4 192.168.1.1/32
```

The following example prevents sequence 1 of the *MyFilter* filter from dropping packets based on destination IP packets:

```
admin@Switch# delete firewall filter MyFilter sequence 1 from destination-address-ipv4
Deleting:
>   destination-address-ipv4: 192.168.1.1/32
OK
```

set firewall filter sequence from destination-address-ipv6

To configure a filter sequence to match packets based on the destination IPv6 address, use the **set firewall filter sequence from destination-address-ipv6** command in L2/L3 configuration mode. To remove the destination IPv6 address, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from destination-address-ipv6** *ipv6-address/mask*
delete firewall filter *filter-name* **sequence** *number* **from destination-address-ipv6**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
ipv6-address/mask	IPv6 address and prefix length.

Example

The following example configures sequence 2 of the *MyFilter* filter to match packets with IPv6 destination address 2001::1/32:

```
admin@Switch# set firewall filter MyFilter sequence 2 from destination-address-ipv6 2001::1/128
```

The following example removes IPv6 destination address 2001::1/32 from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from destination-address-ipv6
Deleting:
>   destination-address-ipv6: 2001::1/128
OK
```

set firewall filter sequence from destination-mac-address

To configure a filter sequence to match packets based on destination MAC address, use the **set firewall filter sequence from destination-mac-address** command in L2/L3 configuration mode. To remove the destination MAC address, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from destination-mac-address** <*mac-address*>
delete firewall filter *filter-name* **sequence** *number* **from destination-mac-address**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
mac-address	Destination MAC address.

Example

The following example configures sequence 2 of the *MyFilter* filter to match packets with destination MAC address 44:44:44:44:44:44:

```
admin@XorPlus# set firewall filter MyFilter sequence 2 from destination-mac-address 44:44:44:44:44:44
```

The following example removes the destination MAC address 44:44:44:44:44:44 from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from destination-mac-address
Deleting:
>   destination-mac-address: 44:44:44:44:44:44
OK
```

set firewall filter sequence from destination-port

To configure a filter sequence to match packets based on destination port, use the **set firewall filter sequence from destination-port** command in L2/L3 configuration mode. To remove the destination port, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from destination-port** *port*
delete firewall filter *filter-name* **sequence** *number* **from destination-port**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
port	Destination port number or port number range, for example, 5000 or 7000..7050.

Example

The following example configures sequence 2 of the *MyFilter* filter to match packets, which destination ports are in the 100-200 range:

```
admin@Switch# set firewall filter MyFilter sequence 2 from destination-port 100..200
```

The following example removes the 100-200 port range from sequence 2 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from destination-port
Deleting:
>   destination-port: 100..200
OK
```

set firewall filter sequence from ether-type

To configure a filter sequence to match packets based on the EtherType field in the Ethernet frame, use the **set firewall filter sequence from ether-type** command in L2/L3 configuration mode. To remove the EtherType field from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from ether-type** *ether-type*
delete firewall filter *filter-name* **sequence** *number* **from ether-type**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
ether-type	EtherType value in decimal form. The range is 0-65535.

Example

The following example configures sequence 2 of the *MyFilter* filter to match frames with EtherType value 0x0800 (2048 decimal):

```
admin@XorPlus# set firewall filter MyFilter sequence 2 from ether-type 2048
```

The following example removes the EtherType value from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from ether-type
Deleting:
>   ether-type: 2048
OK
```

set firewall filter sequence from ip trust-mode

To filter a packet with DSCP or IP Precendence in the packet header, use the **set firewall filter sequence from ip trust-mode** command in L2/L3 coniguration mode. To delete the configuration of firewall filter with DSCP or IP Precendence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from ip trust-mode** { **dscp** | **inet-precendence** }
delete firewall filter *filter-name* **sequence** *number* **from ip trust-mode**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
dscp	Set the firewall filter condition to DSCP (Differentiated Services Code Point).
inet-precendence	Set the firewall filter condition to IP Precedence.

Usage Guidelines

When the firewall filter condition is configured to **dscp** or **inet-precendence**, you need to use the command set firewall filter sequence from ip value to configure the specific value of DSCP or IP Precedence.

These configurations are only used for filtering traffic based on DSCP or IP Precedence values in the packet header but have nothing to do with trust port.

Examples

The following example configures sequence 2 of the *MyFilter* filter to trust DSCP value in the packet header:

```
admin@Switch# set firewall filter MyFilter sequence 2 from ip trust-mode dscp
```

The following example removes the DSCP value from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from ip trust-mode
Deleting:
>   trust-mode: "dscp"
OK
```

set firewall filter sequence from ip value

To configure a filter sequence to match packets based on DSCP or IP Precendence values, use the **set firewall filter sequence from ip value** command in L2/L3 configuration mode.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from ip value** *value*

delete firewall filter *filter-name* **sequence** *number* **from ip**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
value	DSCP or IP Precendence value, according to the trust mode configured with the set firewall filter sequence from ip trust-mode command. The range is 0-7 for IP Precedence, and 0-63 for DSCP.

Examples

The following example configures the trust mode for sequence 2 of *MyFilter* filter to DSCP. The DSCP value used to match packets is then set to 2.

```
admin@Switch# set firewall filter MyFilter sequence 2 from ip trust-mode dscp
admin@Switch# set firewall filter MyFilter sequence 2 from ip value 2
```

The following example removes the trust mode and DSCP value from sequence 2 of *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from ip
Deleting:
>   ip {
>       trust-mode: "dscp"
>       value: 2
>   }
OK
```

set firewall filter sequence from protocol icmp

To configure a filter sequence to match ICMP (Internet Control Message Protocol) packets, use the **set firewall filter sequence from protocol icmp** command in L2/L3 configuration mode.

> **set firewall filter sequence from protocol icmp** and **set firewall filter sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter sequence from protocol others** command with the protocol number.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol icmp** [**type** *type* | **code** *code*]
delete firewall filter *filter-name* **sequence** *number* **from protocol icmp** [**type** | **code**]

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
type	ICMP type. The range is 0-254.
code	ICMP code. The range is 0-254.

Examples

The following example configures sequence 10 of the *MyFilter* filter to match packets with 0 as the ICMP code and 24 as the ICMP type:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol icmp code 0
admin@Switch# set firewall filter MyFilter sequence 10 from protocol icmp type 24
```

The following example removes the match conditions from sequence 10 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 10 from protocol icmp code
Deleting:
>   code: 0
OK
admin@XorPlus# delete firewall filter MyFilter sequence 10 from protocol icmp type
Deleting:
>   type: 24
OK
```

set firewall filter sequence from protocol igmp

To configure a filter sequence to match packets encapsulating IGMP as the Layer 4 protocol, use the **set firewall filter sequence from protocol igmp** command in L2/L3 configuration mode.

> **set firewall filter sequence from protocol icmp** and **set firewall filter sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter sequence from protocol others** command with the protocol number.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol igmp**

delete firewall filter *filter-name* **sequence** *number* **from protocol**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.

Examples

The following example configures sequence 10 of the filter named *MyFilter* to match packets with IGMP as the Layer 4 protocol:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol igmp
```

set firewall filter sequence from protocol ip

To configure a filter sequence to match IP (Internet Porotocol) packets, use the **set firewall filter sequence from protocol ip** command in L2/L3 configuration mode. To remove IP packet matching from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol ip**
delete firewall filter *filter-name* **sequence** *number* **from protocol**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.

Examples

The following example configures sequence 10 of the *MyFilter* filter to match IP packets:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol ip
```

The following example removes the condition that matches IP packets from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol
Deleting:
>   protocol {
>       ip {
>       }
>   }
OK
```

set firewall filter sequence from protocol ospf

To configure a filter sequence to match OSPF (Open Shortest Path First) protocol packets, use the **set firewall filter sequence from protocol ospf** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol ospf**
delete firewall filter *filter-name* **sequence** *number* **from protocol**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.

Examples

The following example configures sequence 10 of the *MyFilter* filter to match OSPF protocol packets:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol ospf
```

The following example removes the condition from sequence 10 of the *MyFilter* fitler:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol
Deleting:
>   protocol {
>       ospf {
>       }
>   }
OK
```

set firewall filter sequence from protocol others

To configure a filter sequence to match packets with the specified Layer 4 protocol number, use the **set firewall filter sequence from protocol others** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol others** *protocol-number*
delete firewall filter *filter-name* **sequence** *number* **from protocol**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range s 0-9999.
protocol-number	Layer 4 protocol number. The range is 0-255.

Examples

This example configures sequence 10 of the *MyFilter* filter to match packets carrying Layer 4 protocol number 21:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol others 21
```

The following example removes the condition from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol
```

set firewall filter sequence from protocol tcp

To configure a filter sequence to match packets with TCP (Transmission Control Protocol) as the Layer 4 protocol, use the **set firewall filter sequence from protocol tcp** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol tcp**
delete firewall filter *filter-name* **sequence** *number* **from protocol**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.

Examples

The following example configures sequence 10 of the *MyFilter* filter to match packets carrying TCP as the Layer 4 protocol:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol tcp
```

The following example removes the condition from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol
Deleting:
>   protocol {
>       tcp {
>       }
>   }
OK
```

set firewall filter sequence from protocol tcp flags

To configure a filter sequence to match packets with TCP as Layer 4 protocol and the specified TCP flag type, use the **set firewall filter sequence from protocol tcp flags** command in L2/L3 configuration mode.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol tcp flags** *type* { **true** | **false** }
delete firewall filter *filter-name* **sequence** *number* **from protocol tcp flags** *type*

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
type	TCP flag type. Possible values are: **ack** **fin** **psh** **rst** **syn** **tcp-established** **tcp-initial urg**
true	The flag is set (1).
false	The flag is not set (0).

Examples

The following example configures sequence 10 of the *MyFilter* filter to match packets with TCP as the Layer 4 protocol and specified values for TCP flags:

```
admin@Switch# set firewall filter MyFilter sequence 1 from protocol tcp flags ack true
admin@Switch# set firewall filter MyFilter sequence 1 from protocol tcp flags psh false
```

The following example removes both match conditions from sequence 1 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 1 from protocol tcp flags ack
Deleting:
>   ack: true
OK
admin@Switch# delete firewall filter MyFilter sequence 1 from protocol tcp flags psh
Deleting:
>   psh: false
OK
```

set firewall filter sequence from protocol udp

To configure a filter sequence to match packets with UDP (User Datagram Protocol) as Layer 4 protocol, use the **set firewall filter sequence from protocol udp** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** from of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from protocol udp**

delete firewall filter *filter-name* **sequence** *number* **from protocol**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.

Examples

The following example configures sequence 10 of the *MyFilter* filter to match packets carrying UDP as Layer 4 protocol:

```
admin@Switch# set firewall filter MyFilter sequence 10 from protocol udp
```

The following example removes the condition from sequence 10 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 from protocol
Deleting:
>   protocol {
>       udp {
>       }
>   }
OK
```

set firewall filter sequence from source-address-ipv4

To configure a filter sequence to match packets with specified source IP address, use the **set firewall filter sequence from source-address-ipv4** command in L2/L3 configuration mode. To remove the condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from source-address-ipv4** *address/prefix-length*
delete firewall filter *filter-name* **sequence** *number* **from source-address-ipv4**

Parameters

filter-name	Filter name.
number	The filter sequence number. The range is 0-9999.
address/prefix-length	IPv4 address / prefix length

Examples

The following example configures sequence 1 of the *MyFilter* filter to match packets with source address 192.168.1.1:

```
admin@Switch# set firewall filter MyFilter sequence 1 from source-address-ipv4 192.168.1.1/32
```

The following example removes the condition from sequence 1 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 1 from source-address-ipv4
Deleting:
>   source-address-ipv4: 192.168.1.1/32
OK
```

set firewall filter sequence from source-address-ipv6

To configure a filter sequence to match packets with specified destination IPv6 address, use the **set firewall filter sequence from source-address-ipv6** command in L2/L3 configuration mode. To remove the condition, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from source-address-ipv6** *address/prefix-length*
delete firewall filter *filter-name* **sequence** *number* **from source-address-ipv6**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
address/prefix-length	IPv6 address / prefix length.

Examples

The following example configures sequence 2 of the *MyFilter* filter to match packets with source IPv6 address is 2001::1:

```
admin@Switch# set firewall filter MyFilter sequence 2 from source-address-ipv6 2001::1/128
```

The following example removes the match condition from sequence 2 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from source-address-ipv6
Deleting:
>   source-address-ipv6: 2001::1/128
OK
```

set firewall filter sequence from source-mac-address

To configure a filter sequence to match packets with the specified source MAC address, use the **set firewall filter sequence from source-mac-address** command in L2/L3 configuration mode.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from source-mac-address** *mac-address*
delete firewall filter *filter-name* **sequence** *number* **from source-mac-address**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
mac-address	Source MAC address.

Examples

The following example configures seqence 2 of the *MyFilter* filter to match packets with the source MAC address 11:22:33:44:55:66:

```
admin@Switch# set firewall filter MyFilter sequence 2 from source-mac-address 11:22:33:44:55:66
```

The following example removes the match condition from sequence 2 of the *MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 2 from source-mac-address
Deleting:
>   source-mac-address: 11:22:33:44:55:66
OK
```

set firewall filter sequence from source-port

To configure a filter sequence to match packets with the specified source port, use the **set firewall filter sequence from source-port** command in L2/L3 configuration mode. To remove the match condition from the filter sequence, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from source-port** *port-number*
delete firewall filter *filter-name* **sequence** *number* **from source-port**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
port-number	Source port number or port number range, for example, 5000 or 7000..7050.

Examples

The following example configures sequence 2 of the *MyFilter* filter to match packets with source port in the 100-234 range:

```
admin@XorPlus# set firewall filter MyFilter sequence 2 from source-port 100..234
```

The following example removes the **souce-port** match condition from sequence 2 of the *MyFilter* filter:

```
admin@XorPlus# delete firewall filter MyFilter sequence 2 from source-port
Deleting:
>   source-port: 100..234
OK
```

set firewall filter sequence from vlan

To configure a filer sequence to filter packets in a specific VLAN, use the **set firewall filter sequence from vlan** command in L2/L3 configuration mode.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **from vlan** *vlan-id*
delete firewall filter *filter-name* **sequence** *number* **from vlan**

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
vlan-id	VLAN identifier. The range is 1-4094.

Example

The following example applies sequence 2 of *MyFilter* filter to VLAN 3:

```
admin@Switch# set firewall filter MyFilter sequence 2 from vlan 3
admin@Switch# commit
admin@Switch# delete firewall filter MyFilter sequence 2 from vlan
admin@Switch# commit
```

set firewall filter sequence then action

To configure the next action for a filter sequence, use the **set firewall filter sequence then action** command in L2/L3 configuration mode.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **then action** { **discard** | **forward** }

Parameters

filter-name	Filter name.
number	Filter sequence number. The range is 0-9999.
discard	Discard packets that meet all match conditions.
forward	Forward packets that meet all match conditions.

Examples

The following example configures sequence 1 and 2 of the *MyFilter* filter to forward and discard matching packets, respectively.

```
admin@Switch# set firewall filter MyFilter sequence 1 then action forward
admin@Switch# set firewall filter MyFilter sequence 2 then action discard
```

set firewall filter sequence then forwarding-class

The **set firewall filter sequence then forwarding-class** command sets forwarding class of ACL rule.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then forwarding-class** <*forwarding-class-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Specifies filter name, the value is a string type, spaces are not allowed.
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
forwarding-class <*forwarding-class-name* >	Specifies forwarding class name, the value is a string type, spaces are not allowed.

Usage Guidelines

After configuring a forwarding class, user could use the **set class-of-service forwarding-class local-priority** command to set mapping between forwarding class and local priority.

Example

Set sequence number 51 to forwarding class class7.

```
admin@Xorplus# set firewall filter f1 sequence 51 then forwarding-class class7
```

set firewall filter sequence log interval

To configure the log interval for a filter sequence, use the **set firewall filter sequence log interval** in L2/L3 configuration mode. To remove the log interval, use the **delete** form of the command.

Command Syntax

set firewall filter *filter-name* **sequence** *number* **log interval** *time*
delete firewall filter *filter-name* **sequence** *number* **log interval**

Parameters

filter-name	Filter name
number	Sequence number. The range is 0-9999.
time	Log interval in seconds.

Example

The following example configures sequence 10 of the *MyFilter* filter to record the log every 15 seconds:

```
admin@Switch# set firewall filter MyFilter sequence 10 log interval 15
```

The following example removes the log interval from sequence 10 of *the MyFilter* filter:

```
admin@Switch# delete firewall filter MyFilter sequence 10 log interval
Deleting:
>   interval: 15
OK
```

set firewall system-output disable

To prevent the switch from filtering packets originating from the switch itself, use the **set firewall system-output disable** command in L2/L3 configuration mode.

Command Syntax

set firewall system-out disable { **true** | **false** }

Parameters

true	Do not apply output filters to traffic from the system itself.
false	Apply output filters to traffic from the system itself.

Example

This example configures the firewall to filter packets originating from the system:

```
admin@Switch# set firewall system-output disable true
```

set firewall time-range periodic start

The **set firewall time-range periodic start** command configures the starting time of a time range.

The **delete firewall time-range periodic start** command deletes the configuration.

Command Syntax

set firewall time-range <*time-range-name*> **periodic** <*periodic*> <**daily** | **friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend**> **start** <*starting-time*>

Parameters

Parameter	Description
time-range <*time-range-name***>**	Specifies the time range name. The value is a string in alpha-numeric format with no spaces.
periodic <*periodic*>	Specifies the periodic name. The value is an integer. Range: 0 to 9999.
<**daily**	**friday	monday	saturday	sunday	thursday	tuesday	wednesday	weekdays	weekend**>	Specifies the days of the week.
start <*starting-time*>	Specifies the starting time of a time range in 24-hour clock format. Format: HH:MM:SS.

Usage Guidelines

NOTEs:

- A pair of start time and end time forms a time range.
- Currently only one **periodic** can be configured under a **time range**. However, multiple time periods can be configured under one **periodic**. All the time periods under the same time range take effect.
- In the same **periodic**, you cannot configure **daily**, **weekdays**, **weekend** at the same time.

```
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays start 8:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays end 18:00:00
admin@Xorplus# commit
Commit OK.
Save done.
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily start 1:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily end 3:00:00
admin@Xorplus# commit
'daily', 'weekdays', 'weekend' should be configured separately in one periodic
Commit failed.
```

Example

- Configure a time range named timerange1234 of weekdays from 8:00:00 to18:00:00.

```
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays start 8:00:00
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays end 18:00:00
admin@Xorplus# commit
```

set firewall time-range periodic end

The **set firewall time-range periodic end** command configures the ending time of a time range.

The **delete firewall time-range periodic end** command deletes the configuration.

Command Syntax

set firewall time-range <*time-range-name*> **periodic** <*periodic*> <**daily** | **friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend**> **end** <*ending-time*>

Parameters

Parameter	Description
time-range <*time-range-name***>**	Specifies the time range name. The value is a string in alpha-numeric format with no spaces.
periodic <*periodic*>	Specifies the periodic name. The value is an integer. Range: 0 to 9999.
<**daily**	**friday	monday	saturday	sunday	thursday	tuesday	wednesday	weekdays	weekend**>	Specifies the days of the week.
end <*ending-time*>	Specifies the ending time of a time range in 24-hour clock format. Format: HH:MM:SS.

Usage Guidelines

NOTEs:

- A pair of start time and end time forms a time range.
- Currently only one **periodic** can be configured under a **time range**. However, multiple time periods can be configured under one **periodic**. All the time periods under the same time range take effect.
- In the same **periodic**, you cannot configure **daily**, **weekdays**, **weekend** at the same time.

```
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays start 8:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 weekdays end 18:00:00
admin@Xorplus# commit
Commit OK.
Save done.
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily start 1:00:00
admin@Xorplus# set firewall time-range time_range3 periodic 1 daily end 3:00:00
admin@Xorplus# commit
'daily', 'weekdays', 'weekend' should be configured separately in one periodic
Commit failed.
```

Example

- Configure a time range named timerange1234 of weekday from 8:00:00 to18:00:00.

```
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays start 8:00:00
admin@Xorplus# set firewall time-range timerange1234 periodic 400 weekdays end 18:00:00
admin@Xorplus# commit
```

run show filter

The command displays information about all filters or a specified filter.

Command Syntax
run show filter [*<filter-name>]*

Parameter
• *<filter-name>* Optional. Specifies a filter name.

Example
• This example shows all filter information:

```
admin@XorPlus# run show filter
Filter: f1
Description: asa
Input interface: ge-1/1/1
Filter: f2
Description:
Input interface: vlan2
Filter: f3
Description:
Output interface: ge-1/1/2
Filter: f4
Description:
Output interface: vlan2
• Show filter f1
XorPlus# run show filter f1
Filter: f1
Description: asa
Input interface: ge-1/1/1
```

- This example shows an ACL-based ERSPAN information:

```
admin@Xorplus# run show filter f1
Filter: f1
    Description:
    Sequence: 1
        Description:
        match counter:  751233 packets
        match-condition:
            protocol:                tcp
            source-address-ipv4:     1.1.1.100/32
        action: forward
        Erspan Output:
               state: UP
               source-ip: 172.1.1.100
               dest-ip: 192.1.1.100
               output-port: te-1/1/2
               tagged vlan:
               vrf:
               ttl: 255
        forwarding_class:
    Input interface: te-1/1/1
```

run show timerange

The **run show timerange** command is used to view the time range configuration information.

Command Syntax

run show timerange [<*time-range-name*>]

Parameter

Parameter	Description
<*time-range-name*>	Optional. Specifies a time range name. The value is a string.

Example

- View the time range configuration information.

```
admin@Xorplus# run show timerange timerange4
TimeRange: timerange4
Periodic: 4
    Week: thursday, start:15:00:00, end:15:10:00

admin@Xorplus# run show timerange
TimeRange: time_range1
Periodic: 0
    Week: daily, start:16:10:00, end:16:15:00
TimeRange: time_range2
Periodic: 1
    Week: friday, start:05:00:00, end:05:10:00
    Week: monday, start:01:25:00, end:01:30:00
    Week: thursday, start:04:10:00, end:04:15:00
    Week: tuesday, start:15:53:00, end:15:54:00
    Week: wednesday, start:00:00:00, end:02:41:00
Periodic: 8881
    Week: friday, start:13:00:00, end:13:10:00
```

QoS Configuration Commands

This section contains descriptions of the Layer2 and Layer3 QoS configuration commands that this chapter references.

- class-of-service classifier <classifier-name>
- class-of-service classifier <classifier-name> forwarding-class <forwarding-class-name> code-point <code-point>
- class-of-service classifier <classifier-name> trust-mode <trust-mode>
- class-of-service forwarding-class <forwarding-class-name> local-priority <local-priority>
- class-of-service interface <port> classifier <classifier-name>
- class-of-service scheduler <scheduler-name> guaranteed-rate <guaranteed-rate>
- class-of-service scheduler <scheduler-name> mode SP
- class-of-service scheduler <scheduler-name> mode WFQ
- class-of-service scheduler <scheduler-name> mode WRR
- class-of-service scheduler <scheduler-name> weight <weight-id>
- class-of-service scheduler-profile <scheduler-profile-name> forwarding-class <forwarding-class-name> schedule <schedule-name>
- show class-of-service <text>
- set class-of-service interface scheduler-profile
- class-of-service interface <port> default-priority <default-priority-type> <default-priority-int>
- class-of-service pfc-profile <profile-name> code-point <code-point> drop <boolean>
- class-of-service interface <port> pfc-profile <profile-name>
- set firewall filter sequence then dscp
- set class-of-service scheduler max-rate
- CoPP Commands
  - set class-of-service forwarding-class local-priority
  - set class-of-service scheduler max-bandwidth-pps
  - set class-of-service scheduler min-bandwidth-pps
  - set class-of-service scheduler-profile copp-profile forwarding-classs scheduler
  - set class-of-service scheduler weight
  - set firewall filter copp sequence from destination-address-ipv4
  - set firewall filter copp sequence from destination-address-ipv6
  - set firewall filter copp sequence from destination-mac-address
  - set firewall filter copp sequence from destination-port
  - set firewall filter copp sequence from ether-type
  - set firewall filter copp sequence from protocol
  - set firewall filter copp sequence from source-address-ipv4
  - set firewall filter copp sequence from source-address-ipv6
  - set firewall filter copp sequence from source-mac-address
  - set firewall filter copp sequence from source-port
  - set firewall filter copp sequence from vlan
  - set firewall filter copp sequence then forwarding-class
  - set firewall filter copp sequence then dscp
  - run show copp bandwidth
  - run show copp statistics
  - run show filter copp
  - run show interface stm
  - run clear copp statistics
- Buffer Management Commands
  - set interface ethernet-switching-options buffer egress-queue shared-ratio
  - set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared
  - run show gigabit-ethernet egress-queues
  - run show interface egress-buffer
- Interface-based Rate Limiting Commands
  - set interface gigabit-ethernet rate-limiting ingress kilobits
  - set interface gigabit-ethernet rate-limiting ingress ratio
  - set interface gigabit-ethernet rate-limiting ingress burst
  - set interface gigabit-ethernet rate-limiting egress kilobits
  - set interface gigabit-ethernet rate-limiting egress ratio
  - set interface gigabit-ethernet rate-limiting egress burst
- ACL-based Traffic Policer Commands
  - set firewall policer if-exceeding count-mode
  - set firewall policer if-exceeding rate-limit
  - set firewall policer if-exceeding burst-limit
  - set firewall filter sequence then policer
  - set firewall policer if-exceeding action discard

    - run show policer
- PFC Watchdog
    - set class-of-service pfc-watchdog granularity
    - set class-of-service pfc-watchdog restore-action
    - set class-of-service pfc-watchdog code-point detect-interval
    - set class-of-service pfc-watchdog code-point restore-interval
    - set class-of-service interface pfc-watchdog code-point enable
    - run show pfc-watchdog config
    - run show pfc-watchdog stats

class-of-service classifier <classifier-name>

User can configure classifier-name for a classifier, and the name is optionally implemented.

Command Syntax
set class-of–service classifier <*classifier-name*>
delete class-of–service classifier c1

Parameter
• <*classifier-name* > Classifier configuration,it is optionally implemented.

Example
• This example creates classifier c1:

```
admin@XorPlus# set class-of-service classifier c1
admin@XorPlus# commit
```

class-of-service classifier <classifier-name> forwarding-class <forwarding-class-name> code-point <code-point>

User can configure a name for a classifier. This name can be applied in an input interface.

Command Syntax

set class-of–service forwarding-class <*forwarding-class-name*> local-priority <*int*>

delete class-of–service classifier c1 forwarding-class f1 code-point 6

Parameter

<*forwarding-class-name*> Name of forwarding class.

<*int*> code-point , the valid range is 0~7 for ieee-802.1 and inet-precedence, 0~63 for dscp.

Example

This example creates a classifier c1 with forwarding-class f1 and code-point 3

```
admin@XorPlus# set class-of-service classifier c1 forwarding-class f1 code-point 3
admin@XorPlus# commit
```

class-of-service classifier <classifier-name> trust-mode <trust-mode>

User can configure classifier-name for a classifier, and the name is optionally implemented.
The value of trust-mode can be DSCP, IEEE 802.1p, or inet-precedence.

Command Syntax
set class-of–service classifier <*classifier-name*> trust-mode <*trust-mode*>
delete class-of–service classifier c1 trust-mode

Parameter
• <*classifier-name* > Classifier configuration. It is optionally implemented.
• <*trust-mode* > Priority based. The value of trust-mode can be DSCP, IEEE 802.1p, or inet-precedence.

Example
• This example creates classifier c1 based on the trust-mode of DSCP:

```
admin@XorPlus# set class-of-service classifier c1 trust-mode dscp
admin@XorPlus# commit
```

• This example creates classifier c2 based on the trust-mode of IEEE 802.1p:

```
admin@XorPlus# set class-of-service classifier c2 trust-mode ieee 802.1p
admin@XorPlus# commit
```

• This example creates classifier c3 based on the trust-mode of inet-precedence:

```
admin@XorPlus# set class-of-service classifier c3 trust-mode inet-precedence
admin@XorPlus# commit
```

class-of-service forwarding-class <forwarding-class-name> local-priority <local-priority>

User can configure the local-priority for a special forwarding-class. The name of a forwarding-class is optionally implemented.

Command Syntax
set class-of–service forwarding-class <*forwarding-class-name*> local-priority <*int*>
delete class-of–service forwarding-class f1 local-priority
delete class-of-service forwarding-class f1

Parameter
• <*forwarding-class-name*> Name of forwarding class.
• <*int*> Local priority,the valid local priority numbers range 0-7.

- Default value: 0

> **NOTE:**
> On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.

Example
• This example creates a forwarding-class f1and the local priority is 1.

```
admin@XorPlus# set class-of-service forwarding-class f1 local-priority 1
admin@XorPlus# commit
```

class-of-service interface <port> classifier <classifier-name>

User can configure a classifier for port.

Command Syntax
set class-of–service interface <*port*> classifier <*classifier-name*>
delete class-of–service interface ge-1/1/1

Parameter
• <*port*> GigabitEthernet IEEE 802.3z or 802.3ae. e.g. ge-1/1/1.
• <*classifier-name*> Classifier configuration. It is optionally implemented.

Example
• This example creates classifier for port ge-1/1/1.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 classifier c1
admin@XorPlus# commit
```

class-of-service scheduler <scheduler-name> guaranteed-rate <guaranteed-rate>

User can configure the minimum guaranteed bandwith for WFQ queue.

Command Syntax

set class-of–service scheduler <*scheduler-name*> guaranteed-rate <*guaranteed-rate*>

delete class-of–service scheduler s1 guaranteed-rate

Parameter

<*schedule-name*> Queue scheduler configuration, it is optionally implemented.

<*guaranteed-rate*> The minimum guaranteed bandwidth, only for WFQ. The valid guaranteed-rate range 8-40000000.

Example

This example creates scheduler s1 with the minimum guaranteed bandwitdth 100.

```
admin@XorPlus# set class-of-service scheduler s1 guaranteed-rate 100
admin@XorPlus# commit
```

class-of-service scheduler <scheduler-name> mode SP

User can configure a scheduler with SP queue.

Command Syntax

set class-of–service scheduler *<scheduler-name>* mode SP

delete class-of–service scheduler s1

Parameter

<scheduler-name> Queue scheduler configuration. It is optionally implemented.

Example

This example creates scheduler s1 with SP queue.

```
admin@XorPlus# set class-of-service scheduler s1 mode SP
admin@XorPlus# commit
```

class-of-service scheduler <scheduler-name> mode WFQ

User can configure the scheduling mode of associated queues and schedule with WFQ queue.

Command Syntax

set class-of–service scheduler <*scheduler-name*> mode WFQ

delete class-of–service scheduler s1

Parameter

<*scheduler-name*> Queue schedule configuration. It is optionally implemented.

Example

This example creates scheduler s1 with WFQ queue.

```
admin@XorPlus# set class-of-service scheduler s1 mode WFQ
admin@XorPlus# commit
```

class-of-service scheduler <scheduler-name> mode WRR

User can configure a scheduler with WRR queue.

Command Syntax

set class-of–service scheduler <*scheduler-name*> mode WRR

delete class-of–service scheduler s1

Parameter

<*schedule-name*> Queue scheduler configuration. It is optionally implemented.

Example

This example creates scheduler s1 with WRR queue.

```
admin@XorPlus# set class-of-service scheduler s1 mode WRR
admin@XorPlus# commit
```

class-of-service scheduler <scheduler-name> weight <weight-id>

User can configure a scheduling weight of associated queues.

Command Syntax

set class-of–service scheduler <*scheduler-name*> weight <*weight-id*>

delete class-of–service scheduler s1 weight

Parameter

<*schedule-name*> Queue scheduler configuration. It is optionally implemented.

<*weight-id*> The scheduling weight of associated queues. The valid weight numbers range 0-15.

Example

This example creates a scheduling weight of associated queues.

```
admin@XorPlus# set class-of-service scheduler s1 weight 3
admin@XorPlus# commit
```

class-of-service scheduler-profile <scheduler-profile-name> forwarding-class <forwarding-class-name> schedule <schedule-name>

User can configure a schedule of queue and a forwarding class for a special scheduler-profile. This scheduler-profile can be applied on an interface.

Command Syntax

set class-of–service scheduler-profile <scheduler-profile-name> forwarding-class <forwarding-class-name> schedule <schedule-name>

delete class-of–service classifier c1 forwarding-class f1 schedule

Parameter

<scheduler-profile-name> Name of scheduler profile.

<forwarding-class-name> Name of forwarding class.

<schedule-name> Queue schedule configuration.

Example

This example creates a scheduler-profile p1 with the forwarding-class f1 and the schedule s1.

```
admin@XorPlus# set class-of-service scheduler-profile p1 forwarding-class f1 schedule s1
admin@XorPlus# commit
```

show class-of-service <text>

The **show class-of-service** command displays information about QoS configured on switch. User can display the interface, trust-mode, local-priority, queue-schedule, and the code-point information. The default queue-schedule is SP.

Command Syntax

run show class-of-service *<text>*

Parameter

• *<text>* The special information. Options include:

- **Interface:** Show class of service on specified interface

Example

• This example shows class-of-service:

```
admin@XorPlus# run show class-of-service
Interface Trust-mode Local-priority Queue-Schedule Code-points
---------- ---------- ------------- ----------------- -----------
ge-1/1/1 ieee-802.1 3 WRR,5 3
```

set class-of-service interface scheduler-profile

The **set class-of–service interface scheduler-profile** command applies scheduler profile at a switch physical interface.

Command Syntax

set class-of–service interface <*interface-name*> **scheduler-profile** <*scheduler-profile-name*>
delete class-of–service interface <*interface-name*> **scheduler-profile** <*scheduler-profile-name*>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies a switch physical interface. For example, te-1/1/49. **Note:** When the interface name is configured to **inbound-control-plane**, it means applying firewall filter to the incoming packets directed to switch CPU. As this function is substituted by CoPP feature, the value **inbound-control-plane** will have no effect. For details of CoPP, please refer to CoPP Configuration Guide.
scheduler-profile <*scheduler-profile-name*>	Specifies scheduler profile name, the value is a string type, spaces are not allowed.

Example

- Configure scheduler-profile p1 for port ge-1/1/1.

```
admin@Switch# set class-of-service interface ge-1/1/1 scheduler-profile p1
```

class-of-service interface <port> default-priority <default-priority-type> <default-priority-int>

User can configure a default priority for incoming packets on a port. The default-priority acts on incoming packets without a special field which is dscp, ieee-802.1 or inet-precedence.

For example, when trust mode is dscp on an interface, if the incoming packets can't match dscp field, these packets will be transmitted by default-priority configured in the interface. Otherwise, these packets will be transmitted by dscp value.

Traffic class for default priority:

	Untrusted	CoS Trusted	ToS Trusted	DSCP Trusted
Untagged Non-IP	Default CoS (port)	Default CoS (port)	Default ToS (port)	Default DSCP (port)
Untagged IP	Default CoS (port)	Default CoS (port)	ToS (packet)	DSCP (packet)
Tagged Non-IP	Default CoS (port)	CoS (packet)	Default ToS (port)	Default DSCP (port)
Tagged IP	Default CoS (port)	CoS (packet)	ToS (packet)	DSCP (packet)

Command Syntax

set class-of–service interface *<port>* default-priority *<default-priority-type> <default-priority-int>*

delete class-of–service interface ge-1/1/1 default-priority

Parameter

<port> Gigabit Ethernet Interface. e.g. ge-1/1/1.

<default-priority-type> the type of default priority, which can be dscp, ieee 802.1p or inet-precedence. The default value is ieee 802.1p.

<default-priority-int> the value of default priority, the valid range is 0~7 for ieee-802.1 and inet-precedence, 0~63 for dscp. The default value is 0 for dscp, ieee 802.1p or inet-precedence.

Example

When not configuring any trust mode, configure default priority dscp 16 on ge-1/1/1.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 default-priority dscp 16
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1

trust mode : no-trust
Default ieee-802.1 : 0
Default dscp : 16
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

When trust mode is dscp, configure default priority dscp 16 on ge-1/1/2.

```
admin@XorPlus# set class-of-service classifier c1 trust-mode dscp
admin@XorPlus# set class-of-service interface te-1/1/2 classifier c1
```

```
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface te-1/1/2
Interface : te-1/1/2
trust mode : dscp
Default ieee-802.1 : 0
Default dscp : 16
Default inet-precedence : 0
Local-priority   Queue-Schedule                Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps                     0,1,2,3,4,5,6,7
1                SP,0kbps                     8,9,10,11,12,13,14,15
2                SP,0kbps                     16,17,18,19,20,21,22,23
3                SP,0kbps                     24,25,26,27,28,29,30,31
4                SP,0kbps                     32,33,34,35,36,37,38,39
5                SP,0kbps                     40,41,42,43,44,45,46,47
6                SP,0kbps                     48,49,50,51,52,53,54,55
7                SP,0kbps                     56,57,58,59,60,61,62,63
```

class-of-service pfc-profile <profile-name> code-point <code-point> drop <boolean>

The full name of pfc is priority flow control. This command defines pfc works on the specified code point.

Note: Lag interface doesn't support pfc, but it supports flow control now. If lag interface has enabled flow control, and its member port has enabled pfc, pfc is valid and flow control is invalid on this member port because pfc has higher priority than flow control.

Command Syntax

set class-of–service pfc-profile <profile-name> code-point <code-point> drop <boolean>
delete class-of–service pfc-profile <profile-name> code-point <code-point> drop

Parameter

- <profile-name> Profile name, string type.
- <code-point> 0~7 value, only match ieee802.1p field.
- <boolean> Value is true or false. Default value is false. If value is false, priority flow control function is enabled on this code point. Otherwise, priority flow control function is disabled on this code point.

Example

• This example creates a pfc profile without any code point configuration. The default is that pfc is enabled on 0~7 code point.

```
admin@XorPlus# set class-of-service pfc-profile pfc1
admin@XorPlus# set class-of-service interface ge-1/1/1 pfc-profile pfc1
admin@XorPlus# commit
Commit OK.
Save done.
admin@XorPlus# run show class-of-service interface ge-1/1/1
Interface : ge-1/1/1
802.1P         Priority Flow Control
-----------    ---------------------
0              true
1              true
2              true
3              true
4              true
5              true
6              true
7              true
trust mode : no-trust
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule           Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

• This example creates a pfc profile with code point 2 drop true.

```
admin@XorPlus# set class-of-service pfc-profile pfc2 code-point 2 drop true
admin@XorPlus# set class-of-service pfc-profile pfc2 code-point 4 drop true
admin@XorPlus# set class-of-service interface ge-1/1/2 pfc-profile pfc2
```

```
admin@XorPlus# commit
Commit OK.
Save done.

admin@XorPlus# run show class-of-service interface ge-1/1/2
Interface : ge-1/1/2
802.1P         Priority Flow Control
-----------    --------------------
0              true
1              true
2              false
3              true
4              false
5              true
6              true
7              true
trust mode : no-trust
Default ieee-802.1 : 0
Default dscp : 0
Default inet-precedence : 0
Local-priority   Queue-Schedule           Code-points
--------------   -------------------------   ------------------------------
0                SP,0kbps
1                SP,0kbps
2                SP,0kbps
3                SP,0kbps
4                SP,0kbps
5                SP,0kbps
6                SP,0kbps
7                SP,0kbps
```

class-of-service interface <port> pfc-profile <profile-name>

The full name of pfc is priority flow control. This command define pfc is applied in a specified port. Pfc acts on packets entering the port, similar to flow control. But flow control only works on the port. It can't work on the code point.

When flow control has been configured on the port, configure pfc. Because pfc has higher priority than flow control, flow control will become invalid on the port.

Command Syntax

set class-of–service interface <port> pfc-profile <profile-name>

delete class-of–service interface <port> pfc-profile

Parameter

- <port> Physical interface.
- <profile-name> pfc profile name, which has been defined in class-of-service pfc-profile in advance.

Example

This example of a pfc profile applied in a port.

```
admin@XorPlus# set class-of-service interface ge-1/1/1 pfc-profile pfc1
admin@XorPlus# commit
Commit OK.
Save done.
```

set firewall filter sequence then dscp

The **set firewall filter sequence then dscp** command remarks the DSCP priority in packets.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*number*> **then dscp** <*dscp-value*>

Parameter

Parameter	Description
filter <*filter-name*>	Specifies a filter name. The value is a string. If the value is **copp**, it indicates a COPP configuration, please refer to set firewall filter copp sequence then dscp for details.
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
dscp <*dscp-value*>	Specifies a value to remark the DSCP priority in packets. The value is an integer in the range of 0 to 63.

Usage Guidelines

To provide differentiated services based on the DSCP priority, run this command to configure the device to remark the DSCP priority in IP packets in a traffic behavior. The DSCP remark function is enabled only when a remarked DSCP priority is set by the user.

Whether the DSCP remark is applied to the inbound or outbound direction on an interface, the device still processes outgoing packets based on the original priority value in the packets, but all the downstream Layer 3 devices processes the packets based on the remarked priority.

Example

- Remark the DSCP priority in packets to 20.

```
admin@Xorplus# set firewall filter f1 sequence 51 then dscp 20
```

set class-of-service scheduler max-rate

The **set class-of-service scheduler max-rate** command sets the maximum rate for an interface queue.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **max-rate** <*value*>

Parameters

Parameter	Description
scheduler <*scheduler-name*>	Specifies a scheduler name, the value is a string, spaces are not allowed.
max-rate <*value*>	Specifies the maximum rate of an interface queue. The value is an integer, in kbit/s.

Usage Guidelines

Configure the maximum rate on the physical interface egress queue of the packet to adjust the sending rate of the interface, thus preventing congestion on the downstream device. When the transmit rate of packets exceeds the queue-based rate limit, the packets will be discarded.

NOTE:

If both queue-based rate limiting and interface-based rate limiting (configured by the command **set interface gigabit-ethernet** <*port*> **rate-limiting** <**ingress** | **egress**> **kilobits** <*kilobits-ps*>) are configured on an interface, the smaller value of the two will be used for rate limiting.

Example

- Set the maximum rate of 30000 kbit/s for scheduler s3.

```
admin@Xorplus# set class-of-service scheduler s3 max-limit 30000
```

CoPP Commands

This section contains descriptions of the CoPP CLI commands.

Although the realization and commands of CoPP use the QoS module of CoS (Class of Service) and Firewall Filter Rule, but CoPP has its own command line with a fixed keyword **copp**, distinguishing it from the ACL feature.

- run clear copp statistics
- run show copp bandwidth
- run show copp statistics
- run show filter copp
- run show interface stm
- set class-of-service forwarding-class local-priority
- set class-of-service scheduler max-bandwidth-pps
- set class-of-service scheduler min-bandwidth-pps
- set class-of-service scheduler-profile copp-profile forwarding-classs scheduler
- set class-of-service scheduler weight
- set firewall filter copp sequence from destination-address-ipv4
- set firewall filter copp sequence from destination-address-ipv6
- set firewall filter copp sequence from destination-mac-address
- set firewall filter copp sequence from destination-port
- set firewall filter copp sequence from ether-type
- set firewall filter copp sequence from protocol
- set firewall filter copp sequence from source-address-ipv4
- set firewall filter copp sequence from source-address-ipv6
- set firewall filter copp sequence from source-mac-address
- set firewall filter copp sequence from source-port
- set firewall filter copp sequence from vlan
- set firewall filter copp sequence then dscp
- set firewall filter copp sequence then forwarding-class

set class-of-service forwarding-class local-priority

The **set class-of-service forwarding-class local-priority** command sets mapping between forwarding class and local priority, the switch will then send different types of packets to the specific CPU queue.

Command Syntax

set class-of-service forwarding-class <*forwarding-class-name*> **local-priority** <*int*>

Parameter

Parameter	Description
forwarding-class <*forwarding-class-name*>	Specifies forwarding class, the value is a string, spaces are not allowed.
local-priority <*int*>	Specifies local priority corresponding to the CPU queue. The value is an integer that ranges from 0 to 23.

Example

• Set forwarding class copp-class3 to CPU queue 20.

```
admin@XorPlus# set class-of-service forwarding-class copp-class3 local priority 20
admin@XorPlus# commit
```

set class-of-service scheduler max-bandwidth-pps

The **set class-of-service scheduler max-bandwidth-pps** command sets the maximum bandwidth for a CPU queue.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **max-bandwidth-pps** <*value*>

Parameter

Parameter	Description
scheduler <*scheduler-name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.
max-bandwidth-pps <*value*>	Specifies the maximum bandwidth for a CPU queue. The value is an integer. The lower limit of max-bandwidth-pps is 0 and the upper limit of max-bandwidth-pps is the maximum bandwidth that the CPU can receive.

Usage Guidelines

If there is heavy traffic load on the interface caused by malicious attacks or network exceptions, the CPU is overloaded and services are interrupted. User can set a maximum bandwidth value for a CPU queue on the interface to control this problem.

The upper limit of max-bandwidth-pps is different on different platforms. If the configured max-bandwidth-pps value exceeds the maximum bandwidth that the CPU can receive, an error message is displayed with the range of the device supported max-bandwidth-pps. The following shows an example.

```
admin@Xorplus# set class-of-service scheduler s1 max-bandwidth-pps 40000
admin@Xorplus# commit
The maximum bandwidth is form 0 to 200
Commit failed.
```

Example

- Set the maximum bandwidth for a CPU queue to 200 pps.

```
admin@XorPlus# set class-of-service scheduler copp-scheduler3 max-bandwidth-pps 200
admin@XorPlus# commit
```

set class-of-service scheduler min-bandwidth-pps

The **set class-of-service scheduler min-bandwidth-pps** command sets the minimum bandwidth for a CPU queue.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **min-bandwidth-pps** <*value*>

Parameter

Parameter	Description
scheduler <*scheduler-name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.
min-bandwidth-pps <*value*>	Specifies the minimum bandwidth for a CPU queue. The value is an integer.

Usage Guidelines

The total value of min-bandwidth-pps of all activated queues should be less than the CPU-affordable PPS depending on different platforms, which should be the maximum PPS threshold to the CPU.

Example

- Set the minimum bandwidth for a CPU queue to 20 pps.

```
admin@XorPlus# set class-of-service scheduler copp-scheduler4 min-bandwidth-pps 20
admin@XorPlus# commit
```

set class-of-service scheduler-profile copp-profile forwarding-classs scheduler

The **set class-of-service scheduler-profile copp-profile forwarding-classs scheduler** command creates a CoPP scheduler profile.

Command Syntax

set class-of-service scheduler-profile copp-profile forwarding-classs <*forwarding-class-name*> **scheduler** <*scheduler-name*>

Parameter

Parameter	Description
forwarding-class <*forwarding-class-name* >	Specifies forwarding class, the value is a string, spaces are not allowed.
scheduler <*copp-scheduler -name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.

Usage Guidelines

The scheduler profile creates a mapping between the forwarding class and the copp scheduler, which define a scheduling strategy for the CPU queue and the queue shaping policy.

Example

- Create a CoPP scheduler profile.

```
admin@XorPlus# set class-of-service scheduler-profile copp-profile forwarding-classs copp-class3 scheduler copp-sch
admin@XorPlus# commit
```

set class-of-service scheduler weight

The **set class-of-service scheduler weight** command sets scheduler weight for a CPU queue, CoPP uses WRR algorithm for queue scheduling.

Command Syntax

set class-of-service scheduler <*scheduler-name*> **weight** <*value*>

Parameter

Parameter	Description
scheduler <*scheduler-name*>	Specifies a CoPP scheduler name, the value is a string, spaces are not allowed.
weight <*value*>	Specifies scheduler weight. The value is an integer that ranges from 1 to 32, refer to Table 2 for default value of the scheduler weight.

Usage Guidelines

Weighted Round Robin (WRR) algorithm ensures that packets in all the queues are scheduled in turn.

When using WRR scheduling, it is necessary to set weight for each queue. The device schedules queues in turn according to their weight value. A bigger weight value indicates a higher priority.

Note:

It is NOT recommended to use the weight value for CPU queue scheduling due to hardware restrictions.

Example

- Set scheduler weight for copp-scheduler3 to 30.

```
admin@XorPlus# set class-of-service scheduler copp-scheduler3 weight 30
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-address-ipv4

The **set firewall filter copp sequence from destination-address-ipv4** command configures a firewall filter rule based on the destination IPv4 address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-address-ipv4 <*ipv4-address*>	Specifies destination IP, it could be a specific IPv4 address or an IPv4 subnet. For example, 192.168.1.10, 10.1.1.0/24.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-address-ipv4** command to configure a firewall filter rule based on the destination IPv4 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the destination IPv4 address of 10.1.1.0/24.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-address-ipv4 10.1.1.0/24
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-address-ipv6

The **set firewall filter copp sequence from destination-address-ipv6** command configures a firewall filter rule based on the destination IPv6 address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-address-ipv6** <*ipv6-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-address-ipv6 <*ipv6-address*>	Specifies destination IPv6, it could be a specific IPv6 address or an IPv6 subnet. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers. For example, aa00:1002::1, 2001::1/32.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-address-ipv6** command to configure a firewall filter rule based on the destination IPv6 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the destination IPv6 address of 2001::1/128.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-address-ipv6 2001::1/128
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-mac-address

The **set firewall filter copp sequence from destination-mac-address** command configures a firewall filter rule based on the destination MAC address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-mac-address** <*mac-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-mac-address <*mac-address*>	Specifies the destination MAC address. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-mac-address** command to configure a firewall filter rule based on the destination MAC address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the destination MAC address of 00:50:ba:27:be:d2.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-mac-address 00:50:ba:27:be:d2
admin@XorPlus# commit
```

set firewall filter copp sequence from destination-port

The **set firewall filter copp sequence from destination-port** command configures a firewall filter rule based on the destination port for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from destination-port** <*port-number*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-port <*port-number*>	Specifies the destination port number or port number range, for example, 5000 or 7000..7050.

Usage Guidelines

You can run the **set firewall filter copp sequence from destination-port** command to configure a firewall filter rule based on the destination port for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the destination port of 3222.

```
admin@XorPlus# set firewall filter copp sequence 51 from destination-port 3222
admin@XorPlus# commit
```

set firewall filter copp sequence from ether-type

The **set firewall filter copp sequence from ether-type** command configures a firewall filter rule based on the Ether-Type values for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from ether-type** <*ether-type*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
ether-type <*ether-type*>	Specifies an Ether-Type value. The value is an integer in decimal format that ranges from 1501 to 65535.

Usage Guidelines

You can run the **set firewall filter copp sequence from ether-type** command to configure a firewall filter rule based on the Ether-Type for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the Ether-Type value 34525.

```
admin@XorPlus# set firewall filter copp sequence 51 from ether-type 34525
admin@XorPlus# commit
```

set firewall filter copp sequence from protocol

The **set firewall filter copp sequence from protocol** command configures a firewall filter rule based on the protocol type for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from protocol** [**icmp | igmp | ip | ospf | others** <*protocol-number*> | **udp | tcp**]

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
protocol [icmp | igmp | ip | ospf | others <*protocol-number*> **| udp | tcp]**	Specifies a protocol name or a protocol number. Protocol name could be **icmp, igmp, ip, ospf, udp** or **tcp**. Protocol number is an integer that ranges from 0 to 255. For example, 8 for EGP, 9 for IGP, 47 for GRE, 88 for EIGRP, 103 for PIM, and 112 for VRRP.

Usage Guidelines

You can run the **set firewall filter copp sequence from protocol** command to configure a firewall filter rule based on the protocol type for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

BPDU, LLDP, LACP and ARP cannot be classified through the protocol field, as they are not an IP protocol. You can classify these protocol packets in other matching fields, such as destination-mac-address, destination-port and ether-type.

NOTE:

set firewall filter copp sequence from protocol icmp and **set firewall filter copp sequence from protocol igmp** commands configure the firewall filter rules based on the ICMP or IGMP protocol type for only IPv4 traffic classification. To configure the firewall filter rule based on the ICMP or IGMP protocol type for IPv6 traffic classification, use the **set firewall filter copp sequence from protocol others** command with the protocol number.

Example

• Configure a firewall filter rule based on ICMP protocol.

```
admin@XorPlus# set firewall filter copp sequence 51 from icmp
admin@XorPlus# commit
```

set firewall filter copp sequence from source-address-ipv4

The **set firewall filter copp sequence from source-address-ipv4** command configures a firewall filter rule based on the source IPv4 address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from source-address-ipv4** <*ipv4-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
source-address-ipv4 <*ipv4-address*>	Specifies source IP, it could be a specific IPv4 address or an IPv4 subnet. For example, 192.168.1.10, 10.1.1.0/24.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-address-ipv4** command to configure a firewall filter rule based on the source IPv4 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the source IPv4 address of 10.1.1.0/24.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-address-ipv4 10.1.1.0/24
admin@XorPlus# commit
```

set firewall filter copp sequence from source-address-ipv6

The **set firewall filter copp sequence from source-address-ipv6** command configures a firewall filter rule based on the source IPv6 address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from source-address-ipv6** <*ipv6-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
source-address-ipv6 <*ipv6-address*>	Specifies source IPv6, it could be a specific IPv6 address or an IPv6 subnet. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, an X contains 4 hexadecimal numbers. For example, aa00:1002::1, 2001::1/128.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-address-ipv6** command to configure a firewall filter rule based on the source IPv6 address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the source IPv6 address of 2001:a100::1/128.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-address-ipv6 2001:a100::1/128
admin@XorPlus# commit
```

set firewall filter copp sequence from source-mac-address

The **set firewall filter copp sequence from source-mac-address** command configures a firewall filter rule based on the source MAC address for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from source-mac-address** <*mac-address*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
destination-mac-address <*mac-address*>	Specifies the source MAC address. The value is in the format of H:H:H:H:H:H. An H contains 2 hexadecimal numbers.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-mac-address** command to configure a firewall filter rule based on the source MAC address for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the source MAC address of 11:50:ba:27:be:d2.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-mac-address 11:50:ba:27:be:d2
admin@XorPlus# commit
```

set firewall filter copp sequence from source-port

The **set firewall filter copp sequence from source-port** command configures a firewall filter rule based on the source port for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from source-port** <*port-number*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
source-port <*port-number*>	Specifies the source port number or port number range, for example, 5000 or 7000..7050.

Usage Guidelines

You can run the **set firewall filter copp sequence from source-port** command to configure a firewall filter rule based on the source port for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

- Configure a firewall filter rule based on the source port of 3222.

```
admin@XorPlus# set firewall filter copp sequence 51 from source-port 3222
admin@XorPlus# commit
```

set firewall filter copp sequence from vlan

The **set firewall filter copp sequence from vlan** command configures a firewall filter rule based on the VLAN ID for traffic classification.

Command Syntax

set firewall filter copp sequence <*number*> **from vlan** <*vlan-id*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

You can run the **set firewall filter copp sequence from vlan** command to configure a firewall filter rule based on the vlan ID for traffic classification so that the device processes packets matching the same firewall filter rule in the same manner.

Example

• Configure a firewall filter rule based on the VLAN 2.

```
admin@XorPlus# set firewall filter copp sequence 51 from vlan 2
admin@XorPlus# commit
```

set firewall filter copp sequence then forwarding-class

The **set firewall filter copp sequence then forwarding-class** command sets forwarding class of CoPP policy.

Command Syntax

set firewall filter copp sequence <*number*> **then forwarding-class** <*forwarding-class-name*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
forwarding-class <*forwarding-class-name* >	Specifies forwarding class name, the value is a string type, spaces are not allowed.

Usage Guidelines

After configuring a forwarding class, user could use the **set class-of-service forwarding-class local-priority** command to set mapping between forwarding class and local priority.

Example

• Set sequence number 51 to forwarding class copp-class7.

```
admin@XorPlus# set firewall filter copp sequence 51 then forwarding-class copp-class7
admin@XorPlus# commit
```

set firewall filter copp sequence then dscp

The **set firewall filter copp sequence then dscp** command remarks the DSCP priority in packets for COPP.

Command Syntax

set firewall filter copp sequence <*number*> **then dscp** <*dscp-value*>

Parameter

Parameter	Description
sequence <*number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999. The integers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 260, 270 are not allowed to be used for sequence numbers in user-defined CoPP firewall filter rules.
dscp <*dscp-value*>	Specifies a value to remark the DSCP priority in packets. The value is an integer in the range of 0 to 63.

Usage Guidelines

To provide differentiated services based on the DSCP priority, run this command to configure the device to remark the DSCP priority in IP packets in a traffic behavior. The DSCP remark function is enabled only when a remarked DSCP priority is set by the user.

Whether the DSCP remark is applied to the inbound or outbound direction on the CPU interface, the device still processes outgoing packets based on the original priority value in the packets, but all the downstream Layer 3 devices processes the packets based on the remarked priority.

Example

- Remark the DSCP priority in packets to 20 for COPP.

```
admin@Xorplus# set firewall filter copp sequence 51 then dscp 20
```

run show copp bandwidth

The **run show copp bandwidth** command displays the CoPP policy information of forwarding class, including bandwidth information, scheduling information and local priority mapping.

Command Syntax

run show copp bandwidth

Parameter

None.

Example

• Show CoPP policy information of forwarding class.

```
admin@Xorplus# run show copp bandwidth
Forwarding Class  Min-Bandwidth Max-Bandwidth Weight Local-Priority Schedule-Mode
default-class        0            80           8      0              WRR
pim-class            0            80           16     8              WRR
igmp-class           0            80           16     9              WRR
vrrp-class           0            80           16     10             WRR
dhcp-class           0            80           16     11             WRR
rip-class            0            80           16     12             WRR
ospf-class           0            80           16     13             WRR
bgp-class            0            80           16     14             WRR
mlag-mac-sync-class  0            80           16     15             WRR
mlag-class           0            80           16     16             WRR
bfd-class            0            80           16     17             WRR
arp-class            20           80           32     18             WRR
arp-class            20           80           32     19             WRR
lldp-class           20           80           32     20             WRR
lacp-class           20           80           32     21             WRR
bpdu-class           20           80           32     22             WRR
management-class     20           80           12     23             WRR
mvrp-class           100          500          32     24             WRR
erps-class           100          500          32     25             WRR
ripng-class          0            500          16     26             WRR
loopback-detection-class   100    500          32     27             WRR
isis-class           0            80           16     13             WRR
```

run show copp statistics

The **run show copp statistics** command displays the statistics information of the forwarding class, including input and dropped packets and rate.

Command Syntax

run show copp statistics [**active** | **forwarding-class** *forwarding-class-name*]

Parameter

Parameter	Description
active	Optional. Specifies state of the forwarding class. With this parameter, only shows the statistics information of the active forwarding class.
forwarding-class *forwarding-class-name*	Optional. Specifies forwarding class name, the value is a string type, spaces are not allowed.

Example

• Show the statistics information of the forwarding class.

```
admin@Xorplus# run show copp statistics
All Copp Traffic statistics:
Input rate 272 bits/sec, 0 packets/sec
Input Packets.........................1
Input Octets.........................153
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets.........................0

arp-class Traffic statistics:
forwarding-class state: inactive
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................0
Input Octets.........................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets.........................0

copp-class1 Traffic statistics:
forwarding-class state: active
Input rate 0 bits/sec, 0 packets/sec
Input Packets.........................0
Input Octets.........................0
Drop rate 0 bits/sec, 0 packets/sec
Drop Packets.........................0
Drop Octets.........................0

......
```

run show filter copp

The **run show filter copp** command displays the configuration information of all CoPP policies, both pre-defined and user-defined, and match counter.

Command Syntax

run show filter copp

Parameter

None.

Example

• Show the configuration information of all CoPP policies, both pre-defined and user-defined, and match counter.

```
admin@Xorplus# run show filter copp
Filter:copp
      Description:
      Sequence: 10
          Description:
          match counter:  0 packets
          match-condition:
              protocol:                bpdu
          action: forward
          forwarding_class: bpdu-class
          ......
      Sequence: 81
          Description:
          match counter:  0 packets
          match-condition:
              destination-port:        23..23
              protocol:                tcp
          action: forward
          forwarding_class: copp-class3
          ......
      Input interface: inbound-control-plane
```

run show interface stm

The **run show interface stm** command displays the total STM resources that are available and how many STM entries are in use.

Note:

It is allowed to configure the firewall filter rule only when there are available STM resources.

Command Syntax

run show interface stm

Parameter

None.

Example

• Show the information of STM resources.

```
admin@Xorplus# run show interface stm
Total stm resource:
  Share-mode: 5
  number of host routes: 32768
  number of mac unicast addresses: 32768
  number of firewall ingress tables: 896
  number of firewall egress tables: 510
  number of IPv4 unicast routes: 5000
  number of IPv6 unicast routes: 500
Stm resource in use:
  number of firewall ingress tables: 2
  number of firewall egress tables: 29
```

The item **number of firewall egress tables** is used for describing STM resources of CoPP. By default, the value of **number of firewall egress tables** in **Stm resource in use:** is 21 as have been used by the default CoPP configurations.

run clear copp statistics

The **run clear copp statistics** command clears the past statistics information of CoPP policy.

Command Syntax

run clear copp statistics

Parameter

None.

Usage Guidelines

If you want to obtain the latest statistics information of CoPP policy, use this command to clear the past statistics information, When new packets coming, new statistics information is generated.

Example

• Clear the past statistics information of CoPP policy.

```
admin@Xorplus# run clear copp statistics
admin@Xorplus# commit
```

Buffer Management Commands

- set interface ethernet-switching-options buffer egress-queue shared-ratio
- set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared
- run show gigabit-ethernet egress-queues
- run show interface egress-buffer

set interface ethernet-switching-options buffer egress-queue shared-ratio

The **set interface ethernet-switching-options buffer shared-ratio** command sets the dynamic threshold ratio of the available shared space.

Command Syntax

set interface ethernet-switching-options buffer egress-queue <*queue-index*> **shared-ratio** <*ratio-value*>

Parameter

Parameter	Description
egress-queue <*queue-index*>	Specifies the interface queue. The value is an integer that ranges from 0 to 7. NOTE: On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
shared-ratio <*ratio-value*>	Specifies the value of the dynamic threshold ratio of the available shared space. The value is an integer that ranges from 0 to 100, indicating 1% to 100%. The default value is 33.

Usage Guidelines

The dynamic mode of both multicast (must enable dynamic threshold) and unicast queues can configure the max dynamic threshold ratio. The threshold is still dynamically adjusted until reaching the max ratio configured.

For the maximum shared-area ratio for a queue, the percentage values 0 to 100 are divided into 10 rages. The table below shows the effective values that correspond to the configured values of ratio-value.

> **NOTE:**
>
> Currently, multicast queue just support eight (1~67) effective ratio value on all platforms.

Example

- Set the dynamic threshold ratio of the available shared space to 40%.

```
admin@Xorplus# set interface ethernet-switching-options buffer egress-queue 0 shared-ratio 40
admin@Xorplus# commit
```

set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared

The **set interface ethernet-switching-options buffer egress-queue mc-queue-dynamic-shared** command is used to enable or disable the dynamic mode of buffer management of the queue.

Command Syntax

set interface ethernet-switching-options buffer egress-queue <*queue-index*> **mc-queue-dynamic-shared** <**true** | **false**>

Parameter

Parameter	Description
egress-queue <*queue-index*>	Specifies the interface queue. The value is an integer that ranges from 0 to 7. **NOTE:** On Trident and Trident+ based switches, known unicast packets can be assigned to a specific queue between queues from 0 to 7, while unknown unicast packets, multicast packets, and broadcast packets can be assigned to a specific queue between queues from 0 to 3.
mc-queue-dynamic-shared <**true**	**false**>	Enable or disable the dynamic mode of buffer management of the queue. The value could be **true** or **false**. • **true**: enable the dynamic mode of buffer management of the queue. • **false**: disable the dynamic mode of buffer management of the queue. By default dynamic mode of buffer management is disabled.

Usage Guidelines

1. Multicast queue

- static mode: This is the default configuration

The value of the static threshold is configured for the multicast queue in the shared space. This avoids the scenario where the port enabled flow control or PFC affects the forwarding of other ports. But the disadvantage is less efficient use of memory.

- dynamic mode: Need to configure

The memory threshold is adjusted dynamically according to the available shared memory in this mode. The thresholds value will dynamically decrease when the available shared memory decreases. The thresholds will rise up when the available shared memory rises up.

2. Unicast queue

- dynamic mode

Dynamic threshold is the default mode for the unicast queue, and it can't configure static threshold.

Example

- Enable or disable the dynamic mode of buffer management of queue 0.

```
admin@Xorplus# set interface ethernet-switching-options buffer egress-queue 0 mc-queue-dynamic-shared true
admin@Xorplus# commit
```

run show gigabit-ethernet egress-queues

The **run show gigabit-ethernet egress-queues** command displays the traffic statistics on an outbound interface queue.

Command Syntax

run show gigabit-ethernet <*interface-name*> **egress-queues** <*queue-index*>

Parameter

Parameter	Description
gigabit-ethernet <*interface-name*>	Specifies the name of the physical interface. The value is a string.
egress-queue <*queue-index*>	Optional. Specifies the interface queue. The value is an integer that ranges from 0 to 7.

Example

- Display the traffic statistics on an outbound interface queue.

```
admin@Xorplus# run show interface gigabit-ethernet ge-1/1/20 egress-queues 1
OutPackets   :0
OutBytes     :0
DropPackets  :0
DropBytes    :0
UCqueuedBytes:0
MCqueuedBytes:0
UCDepth      :202730
MCDepth      :55328
```

Table 1 Description of the run show gigabit-ethernet egress-queues command output

Item	Description
OutPackets	Number of packets sent by an interface queue.
OutBytes	Number of bytes sent by an interface queue.
DropPackets	Number of packets dropped by an interface queue.
DropBytes	Number of bytes sent by an interface queue.
UCqueuedBytes	Number of unicast bytes buffered by an interface queue.
MCqueuedBytes	Number of multicast bytes buffered by an interface queue.
UCDepth	The total memory space of each queue for unicast bytes.
MCDepth	The total memory space of each queue for multicast bytes.

run show interface egress-buffer

The **run show interface egress-buffer** command displays the configuration information for the buffer management.

Command Syntax

run show interface egress-buffer

Parameter

None.

Example

- Display the configuration information for the buffer management.

```
admin@Xorplus# run show interface egress-buffer
Queue UC-Enabled UC-Shared-Ratio MC-Enabled MC-Shared-Ratio
0     true       33              false      --
1     true       33              false      --
2     true       33              false      --
3     true       33              false      --
4     true       33              false      --
5     true       33              false      --
6     true       33              false      --
7     true       33              false      --
```

Interface-based Rate Limiting Commands

- set interface gigabit-ethernet rate-limiting ingress kilobits
- set interface gigabit-ethernet rate-limiting ingress ratio
- set interface gigabit-ethernet rate-limiting ingress burst
- set interface gigabit-ethernet rate-limiting egress kilobits
- set interface gigabit-ethernet rate-limiting egress ratio
- set interface gigabit-ethernet rate-limiting egress burst

set interface gigabit-ethernet rate-limiting ingress kilobits

The **set interface gigabit-ethernet rate-limiting ingress kilobits** command sets a rate limit value in kbit/s on a port for the ingress traffic.

NOTE:

- In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.
- Tomahawk series switches (including Tomahawk, Tomahawk+, Tomahawk2 and so forth) do not support ingress interface-based rate limiting.

Command Syntax

set interface gigabit-ethernet *<interface-name>* **rate-limiting ingress kilobits** *<value>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value is a string.
kilobits *<value>*	Specifies the rate limit value in kbits/s. The value is an integer that ranges from 0 to 10000000. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 1000 kbit/s on port ge-1/1/1 for the ingress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting ingress kilobits 1000
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting ingress ratio

The **set interface gigabit-ethernet rate-limiting ingress ratio** command sets a rate limit value on a port for the ingress traffic in percentage.

NOTE:

- In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.
- Tomahawk series switches (including Tomahawk, Tomahawk+, Tomahawk2 and so forth) do not support ingress interface-based rate limiting.

Command Syntax

set interface gigabit-ethernet *<interface-name>* **rate-limiting ingress ratio** *<value>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value is a string.
ratio *<value>*	Specifies the rate limit value in percentage of the interface rate. The value is an integer that ranges from 0 to 100. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 10% of the interface rate on ge-1/1/1 for the ingress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting ingress ratio 10
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting ingress burst

The **set interface gigabit-ethernet rate-limiting ingress burst** command sets a burst limit value on a port for the ingress traffic.

> **NOTE**:
>
> Tomahawk series switches (including Tomahawk, Tomahawk+, Tomahawk2 and so forth) do not support ingress interface-based rate limiting.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **rate-limiting ingress burst** <*burst-size*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value is a string.
burst <*burst-size*>	Specifies the burst size in kbit, which is the maximum volume of burst traffic that can pass through an interface. The value is an integer from 1 to the value of interface rate. When burst size is not configured, PICOS uses a burst size adapted according to the configured rate limiting value configured by the **set interface gigabit-ethernet** <*interface-name*> **rate-limiting ingress kilobits** <*value*> or **set interface gigabit-ethernet** <*interface-name*> **rate-limiting ingress ratio** <*value*> command.

Example

- Set the burst size value to 10 kbit on port ge-1/1/1 for the ingress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting ingress burst 10
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting egress kilobits

The **set interface gigabit-ethernet rate-limiting egress kilobits** command sets a rate limit value in kbit/s on a port for the egress traffic.

> **NOTE**:
> In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.

Command Syntax

set interface gigabit-ethernet *<interface-name>* **rate-limiting egress kilobits** *<value>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value is a string.
kilobits *<value>*	Specifies the rate limit value in kbits/s. The value is an integer that ranges from 0 to 10000000. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 1000 kbit/s on port ge-1/1/1 for the egress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting egress kilobits 1000
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting egress ratio

The **set interface gigabit-ethernet rate-limiting egress ratio** command sets a rate limit value on a port for the egress traffic in percentage.

> **NOTE**:
> In the same direction of the same interface, kilobits and ratio cannot be configured simultaneously.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **rate-limiting egress ratio** <*value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value is a string.
ratio <*value*>	Specifies the rate limit value in percentage of the interface rate. The value is an integer that ranges from 0 to 100. When the value is configured to 0, it indicates no rate limit on the interface.

Example

- Set the rate limit value to 10% of the interface rate on ge-1/1/1 for the egress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting egress ratio 10
admin@Xorplus# commit
```

set interface gigabit-ethernet rate-limiting egress burst

The **set interface gigabit-ethernet rate-limiting egress burst** command sets a burst limit value on a port for the egress traffic.

Command Syntax

set interface gigabit-ethernet <*interface-name*> **rate-limiting egress burst** <*burst-size*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value is a string.
burst <*burst-size*>	Specifies the burst size in kbit, which is the maximum volume of burst traffic that can pass through an interface. The value is an integer from 1 to the value of interface rate. When burst size is not configured, PICOS uses a burst size adapted according to the configured rate limiting value configured by the **set interface gigabit-ethernet** <*interface-name*> **rate-limiting egress kilobits** <*value*> or **set interface gigabit-ethernet** <*interface-name*> **rate-limiting egress ratio** <*value*> command.

Example

- Set the burst size value to 10 kbit on port ge-1/1/1 for the egress traffic.

```
admin@Xorplus# set interface gigabit-ethernet ge-1/1/1 rate-limiting egress burst 10
admin@Xorplus# commit
```

ACL-based Traffic Policer Commands

- set firewall policer if-exceeding count-mode
- set firewall policer if-exceeding rate-limit
- set firewall policer if-exceeding burst-limit
- set firewall filter sequence then policer
- set firewall policer if-exceeding action discard
- run show policer

set firewall policer if-exceeding count-mode

The **set firewall policer if-exceeding count-mode** command configures the data rate units for the rate-limit and burst-limit of a policer. The value could be **packet** or **kbit**.

Command Syntax

set firewall policer <*policer-name*> **if-exceeding count-mode** <*count-mode*>

Parameter

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.
count-mode <*count-mode*>	Specifies the count mode for the rate-limit and burst-limit of a policer. The value could be **packet** or **kbit**. • **packet**: packet per second. • **kbit**: kbit per second. By default, the count mode is pps.

Usage Guidelines

When the count mode is **packet**, the range of rate-limit and burst-limit is from 1 to 1000 pps.

When the count mode is **kbit**, the range of rate-limit is from 0 to 100000000 kbit/s, and burst-limit is from 0 to 100000000 kbit.

Example

- Configure the count mode for the rate-limit and burst-limit the policer as **kbit** and use **run show policer** to check the configuration.

```
admin@Xorplus# set firewall policer p1 if-exceeding count-mode kbit
admin@Xorplus# run show policer
Policer     rate limit   burst limit   count mode   action
------------   ----------   ----------    ----------   ----------
p1        5000       0        kbit      discard
```

set firewall policer if-exceeding rate-limit

The **set firewall policer if-exceeding rate-limit** command configures the rate limit value for a policer.

> **NOTE:**
> It is NOT recommended to use the rate limit value for CPU queue due to hardware restrictions.

Command Syntax

set firewall policer <*policer-name*> **if-exceeding rate-limit** <*value*>

Parameters

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.
rate-limit <*value*>	Specifies the rate limit value of a policer. The data rate unit is **set by set firewall policer if-exceeding count-mode** command. • When the count mode is **packet**, the range of rate-limit is from 1 to 1000 pps. • When the count mode is **kbit**, the range of rate-limit is from 0 to 100000000 kbit/s.

Example

- The following example configures rate limiting for the *p1* policer to 100 pps (packets per second):

```
admin@Xorplus# set firewall policer p1 if-exceeding count-mode packet
admin@Xorplus# set firewall policer p1 if-exceeding rate-limit 100
admin@Xorplus# run show policer
Policer     rate limit   burst limit   count mode   action
------------   ----------   ----------    ----------   ----------
p1        100       0         packet      discard
```

set firewall policer if-exceeding burst-limit

The **set firewall policer if-exceeding burst-limit** command configures the burst limit value for a policer.

Command Syntax

set firewall policer <*policer-name*> **if-exceeding burst-limit** <*value*>

Parameters

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.
burst-limit <*value*>	Specifies the burst limit value of a policer. The data rate unit is **set by set firewall policer if-exceeding count-mode** command. • When the count mode is **packet**, the range of burst-limit is from 0 to 1000 pps. • When the count mode is **kbit**, the range of burst-limit is from 0 to 100000000 kbit.

Example

- The following example configures burst limiting for the *p1* policer to 500 pps (packets per second).

```
admin@Xorplus# set firewall policer p1 if-exceeding count-mode packet
admin@Xorplus# set firewall policer p1 if-exceeding burst-limit 500
admin@Xorplus# run show policer
Policer         rate limit   burst limit   count mode  action
------------   ----------  ----------    ----------   ----------
p1              100          500           packet      discard
```

set firewall filter sequence then policer

The **set firewall filter sequence then policer** command configures the policer for packets matching a filter sequence.

Command Syntax

set firewall filter <*filter-name*> **sequence** <*sequence-number*> **then policer** <*policer-name*>

Parameters

Parameter	Description
filter <*filter-name*>	Specifies filter name, the value is a string type, spaces are not allowed.
sequence <*sequence-number*>	Specifies filter sequence number. The value is an integer that ranges from 0 to 9999.
policer <*policer-name*>	Specifies the policer name. The value is a string.

Example

- This example configures sequence 1 of the *MyFilter* filter to match packets with source address 192.168.1.1 and the *MyPolicer* policer to be applied to packets matching the *MyFilter* filter:

```
admin@Switch# set firewall filter MyFilter sequence 1 from source-address-ipv4  192.168.1.1/32
admin@Switch# set firewall filter MyFilter sequence 1 then policer MyPolicer
```

set firewall policer if-exceeding action discard

The **set firewall policer if-exceeding action discard** command configures the action to drop the packets for a policer.

Command Syntax

set firewall policer <*policer-name*> **then action discard**

Parameters

Parameter	Description
policer <*policer-name*>	Specifies the policer name. The value is a string.

Usage Guidelines

When the user configures the rate limit or burst limit of an ACL-based traffic policer, the interface then drops the packets whose rate exceeds the rate limit value so that the traffic rate is limited within a proper range. The default action is discard if not configured.

Example

- Configure the action to drop the packets for a traffic policer.

```
admin@Xorplus# set firewall policer MyPolicer if-exceeding count-mode kbit
admin@Xorplus# set firewall policer MyPolicer if-exceeding rate-limit 5000
admin@Xorplus# set firewall policer p1 then action discard
admin@Xorplus# run show policer
Policer     rate limit   burst limit   count mode   action
------------   ----------   ----------    ----------    ----------
p1        5000         0        kbit       discard
```

run show policer

The **run show policer** command displays the policer configuration information.

Command Syntax

run show policer

Parameter

None.

Example

- Run **run show policer** command to view the policer configuration information.

```
admin@Xorplus# run show policer
policer     rate limit   burst limit   count mode   action
-------------------------------------------------------------------------
 p1        5000          0          kbit      discard
```

PFC Watchdog

- set class-of-service pfc-watchdog granularity
- set class-of-service pfc-watchdog restore-action
- set class-of-service pfc-watchdog code-point detect-interval
- set class-of-service pfc-watchdog code-point restore-interval
- set class-of-service interface pfc-watchdog code-point enable
- run show pfc-watchdog config
- run show pfc-watchdog stats

set class-of-service pfc-watchdog granularity

The **set class-of-service pfc-watchdog granularity** command configures the granularity of the PFC deadlock detection and restore timer.

The **delete class-of-service pfc-watchdog granularity** command restores the default configuration.

Command Syntax

set class-of-service pfc-watchdog granularity <**10** | **100**>

delete class-of-service pfc-watchdog granularity

Parameter

Parameter	Description
granularity <**10** | **100**>	Specifies the granularity of the PFC deadlock detection timer and restore timer. The value could be **10** or **100**, in milliseconds. The default value is 100 ms.

Usage Guidelines

Use this command to adjust the granularity of the PFC deadlock detection timer, thereby controlling the PFC deadlock detection time.

Example

- Configure the granularity of the PFC deadlock detection and restore timer to 10 ms.

```
admin@PICOS# set class-of-service pfc-watchdog granularity 10
admin@PICOS# commit
```

set class-of-service pfc-watchdog restore-action

The **set class-of-service pfc-watchdog restore-action** command configures the restore action after a deadlock is detected on the device.

The **delete class-of-service pfc-watchdog restore-action** command restores the default configuration.

Command Syntax

set class-of-service pfc-watchdog restore-action <**forward** | **drop**>

delete class-of-service pfc-watchdog restore-action

Parameter

Parameter	Description
restore-action <**forward** | **drop**>	Configures the restore action after a deadlock is detected on the device. The value could be **forward** or **drop**. • **forward**: forwards received data packets. • **drop**: drops received data packets. The default value is **forward**.

Usage Guidelines

During the PFC deadlock recovery process, the received PFC PAUSE frame will be ignored, and the internal scheduler will resume forwarding the traffic. It is also possible to configure the system to drop the traffic and restore the normal PFC flow control mechanism after the recovery timer.

Example

- Configure the restore action after a deadlock occurs on the device.

```
admin@PICOS# set class-of-service pfc-watchdog restore-action drop
admin@PICOS# commit
```

set class-of-service pfc-watchdog code-point detect-interval

The **set class-of-service pfc-watchdog code-point detect-interval** command configures the time interval of PFC deadlock detection. The value of detection time depends on the configured **granularity** and **detect-timer**, the value of detection time = **granularity** x **detect-interval**.

The **delete class-of-service pfc-watchdog code-point detect-interval** command restores the default configuration.

Command Syntax

For Trident3 platforms:

set class-of-service pfc-watchdog code-point <*cos*> **detect-interval** <*detect-interval*>

delete class-of-service pfc-watchdog code-point <*cos*> **detect-interval**

For Tomahawk3 platforms:

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **detect-interval** <*detect-interval*>

delete class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **detect-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port or a LAG port.
code-point <*cos*>	Specifies the COS value of the packets. The value is an integer that ranges from 0 to 7.
detect-interval <*detect-interval*>	Specifies the time interval of PFC deadlock detection. The value is an integer that ranges from 1 to 15. The default value is 15.

Usage Guidelines

After receiving the PFC Pause frame, the internal scheduler will stop forwarding the queue traffic of corresponding priority and start the timer to detect the PFC Pause frame received by the queue based on the set deadlock detection and granularity.
If the queue remains under flow control state within the configured PFC deadlock detection time, it is considered that a PFC deadlock has occurred and a PFC deadlock restore process is required.

Example

- Configure the time interval of PFC deadlock detection.

```
admin@PICOS# set class-of-service pfc-watchdog code-point 5 detect-interval 10
```

```
admin@PICOS# commit
```

set class-of-service pfc-watchdog code-point restore-interval

The **set class-of-service pfc-watchdog code-point restore-interval** command configures the restore time when PFC deadlock occurs. The value of restore time depends on the configured **granularity** and **restore-interval**, the restore time = **granularity** x **restore-interval**.

The **delete class-of-service pfc-watchdog code-point restore-interval** command restores the default configuration.

Command Syntax

For Trident3 platforms:

set class-of-service pfc-watchdog code-point <*cos*> **restore-interval** <*restore-interval*>

delete class-of-service pfc-watchdog code-point <*cos*> **restore-interval**

For Tomahawk3 platforms:

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **restore-interval** <*restore-interval*>

delete class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **restore-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port or a LAG port.
code-point <*cos*>	Specifies the COS value of the packets. The value is an integer that ranges from 0 to 7.
restore-interval <*restore-interval*>	Specifies the restore time when PFC deadlock occurs. The value is an integer that ranges from 1 to 15. The default value is 15.

Usage Guidelines

When a PFC deadlock has occurred and a PFC deadlock restore process is required. During the PFC deadlock recovery process, the PFC PAUSE frames received by the port will be ignored, and the internal scheduler will resume sending queue traffic of corresponding priority. It is also possible to choose to drop queue traffic of the corresponding priority and restore normal PFC flow control mechanism after the restore time.

Example

- Configure the restore time when PFC deadlock occurs.

```
admin@PICOS# set class-of-service pfc-watchdog code-point 5 restore-interval 10
admin@PICOS# commit
```

set class-of-service interface pfc-watchdog code-point enable

The **set class-of-service interface pfc-watchdog code-point enable** command enables PFC watchdog functionality.

The **delete class-of-service interface pfc-watchdog code-point enable** command restores the default configuration.

Command Syntax

set class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **enable** <**true** | **false**>

delete class-of-service interface <*interface-name*> **pfc-watchdog code-point** <*cos*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port or a LAG port. The default value is 100 ms.
code-point <*cos*>	Specifies the COS value of the packets. The value is an integer that ranges from 0 to 7.
enable <**true** | **false**>	Enables or disables PFC watchdog functionality. The value could be **true** or **false**. • **true**: enables PFC watchdog functionality. • **false**: disables PFC watchdog functionality. By default, PFC watchdog is disabled.

Example

- Enable PFC watchdog functionality.

```
admin@PICOS# set class-of-service interface ge-1/1/1 pfc-watchdog code-point 5 enable true
admin@PICOS# commit
```

run show pfc-watchdog config

The **run show pfc-watchdog config** command shows the configuration information about PFC watchdog.

Command Syntax

run show pfc-watchdog config

Parameter

Null.

Example

- View the configuration information about PFC watchdog.

```
admin@PICOS# run show pfc-watchdog config
      PORT       ACTION          QUEUE    DETECTION TIME    RESTORATION TIME
----------  -----------   ------------  ----------------  ------------------
te-1/1/25          drop              6               150                 150
                                     7               150                 150
                                     6                80                  70
```

run show pfc-watchdog stats

The **run show pfc-watchdog stats** command shows the statistics information about PFC watchdog, including the number of PFC pause storms that have been detected and restored, as well as the number of packets that have been dropped, on the PFC queues on an interface.

Command Syntax

run show pfc-watchdog stats

Parameter

Null.

Example

- View the statistics information about PFC watchdog.

```
admin@PICOS# run show pfc-watchdog stats
       QUEUE       STATUS    STORM DETECTED/RESTORED        TX OK/DROP    TX LAST OK/DROP
------------  -----------  -------------------------  ----------------  -----------------
te-1/1/25:5       stormed                        9/8      82072626556/0      32053822365/0
te-1/1/25:6       stormed                        9/8      31504345475/0      32053822365/0
te-1/1/25:7   operational                        0/0                0/0                0/0
```

In the show result,

- **STATUS**: The status of PFC watchdog. The value could be **operational** or **stormed**.
  - **operational**: Currently under detection, no deadlock found.
  - **stormed**: Currently in a deadlock state.
- **STORM DETECTED**: Queue deadlock counter.
- **STORM RESTORED**: Queue Restore counter.
- **TX DROP** and **TX LAST DROP**: Number of Tx packets dropped due to PFC deadlock.
- **TX OK** and **TX LAST OK**: Number of Tx packets transmitted during deadlock (Forward action).

Protocol Configuration Commands

- protocols arp aging-time
- set protocols arp interface address mac-address
- set protocols arp interface proxy
- set protocols arp inspection vlan disable
- set protocols arp inspection access-list ip mac-address
- set protocols arp inspection vlan access-list
- set protocols arp inspection trust-port
- run show arp
- run show arp inspection dhcp-binding
- run show arp inspection interface
- run show arp inspection vlan
- run show arp inspection access-list
- run show arp inspection statistics vlan
- protocols lacp interface <interface> priority
- protocols lacp priority
- protocols sflow agent-id
- protocols sflow collector udp-port
- protocols sflow disable
- protocols sflow header-len
- protocols sflow interface <port> disable
- protocols sflow interface <port> header-len
- protocols sflow interface <port> polling-interval
- protocols sflow interface <port> sampling-rate egress
- protocols sflow interface <port> sampling-rate ingress
- protocols sflow polling-interval
- protocols sflow sampling-rate egress
- protocols sflow sampling-rate ingress
- protocols sflow source-address
- set protocols dhcp snooping vlan
- set protocols dhcp snooping trust-port
- set protocols dhcp snooping vlan option82-policy
- set protocols dhcp snooping option82 circuit-id
- set protocols dhcp snooping option82 remote-id
- set protocols dhcp snooping option82 trust-all
- set protocols dhcp snooping binding file
- set protocols dhcp snooping binding write-delay
- run show dhcp snooping binding
- set protocols dhcp relay interface disable
- set protocols dhcp relay interface dhcp-server-address
- set protocols dhcp relay interface relay-agent-address
- set protocols dhcp relay interface option82-policy
- set protocols dhcp relay option82 circuit-id
- set protocols dhcp relay option82 remote-id
- set protocols dhcp relay option82 trust-all
- set protocols dhcp server pool network
- set protocols dhcp server pool range low
- set protocols dhcp server pool range high
- set protocols dhcp server pool domain-name
- set protocols dhcp server pool dns-server
- set protocols dhcp server pool default-router
- set protocols dhcp server pool lease-time
- set protocols dhcp server pool vrf
- run show dhcp server binding address
- run show dhcp server binding interface
- set protocols dhcp6 relay interface disable
- set protocols dhcp6 relay interface destination
- set protocols dhcp6 relay interface remote-id
- run show dhcp6 relay-stats
- set protocols lacp interface rate
- run show lldp neighbor
- set protocols dhcp6 snooping vlan

- set protocols dhcp6 snooping trust-port
- set protocols dhcp6 snooping binding file
- set protocols dhcp6 snooping binding write-delay
- set protocols dhcp6 snooping vlan option-policy
- set protocols dhcp6 snooping option37 remote-id
- set protocols dhcp6 snooping option18 interface-id
- set protocols dhcp6 snooping interface max-clients
- run show dhcp6 snooping binding
- set protocols dhcp6 guard policy device-role
- set protocols dhcp6 guard policy trust-port
- set protocols dhcp6 guard policy interface
- set protocols dhcp6 guard policy preference-min
- set protocols dhcp6 guard policy preference-max
- set protocols dhcp6 guard policy match server source-address
- set protocols dhcp6 guard policy match reply ia-prefix
- run show dhcp6 guard policy
- run show dhcp6 guard

protocols arp aging-time

The Address Resolution Protocol (ARP) maps an IP address to a MAC address to enable communications within an IP network broadcast domain. If a given host (A) does not have the MAC address of another host (B) with which it wants to communicate, the sending host will generate a broadcast message to all hosts within the broadcast domain in order to obtain the MAC address of host B. While all hosts will receive the ARP request, only host B will respond with its MAC address. Host A will then cache the MAC address for future use. ARP aging is used to set the amount of time the address will remain in that cache. The default ARP aging time is 1200 seconds. This document describes how to change the ARP aging time.

Command Syntax
set protocols arp aging-time <*seconds*>
delete protocols arp aging-time

Parameter
•<*seconds*> Aging time in seconds,[300..14400]

Example
• This example is to set arp aging time to 400:

```
admin@XorPlus# set protocols arp aging-time 400
admin@XorPlus# commit
```

set protocols arp interface address mac-address

The **set protocols arp interface address mac-address** command configures a static ARP entry.

Command Syntax
set protocols arp interface <*interface*> **address** <*ipv4-addr*> **mac-address** <*mac-addr*>
delete protocols arp interface <*interface*> **address** <*ipv4-addr*> **mac-address** <*mac-addr*>

Parameter

Parameter	Description
interface <*interface*>	Specifies the outbound interface in a static ARP entry. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
address <*ipv4-addr*>	Specifies the IPv4 address in a static ARP entry.
mac-address <*mac-addr*>	Specifies the MAC address in a static ARP entry.

Example

- Configure a static ARP entry that maps the IP address 10.10.60.1 to the MAC address 22:11:11:11:11:11.

```
admin@XorPlus# set protocols arp interface vlan4 address 10.10.60.1 mac-address 22:11:11:11:11:11
admin@XorPlus# commit
```

set protocols arp interface proxy

The **set protocols arp interface proxy disable** command can be used to enable or disable proxy ARP on an interface.

Command Syntax
set protocols arp interface <*interface*> **proxy disable <true | false>**
delete protocols arp interface <*interface*> **proxy**

Parameter

Parameter	Description
interface <*interface*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
disable <true | false>	Enables or disables proxy ARP. The value could be **true** or **false**. • **true**: Disables proxy ARP. • **flase**: Enables proxy ARP.

Example

- Enable proxy ARP on vlan4:

```
admin@XorPlus# set protocols arp interface vlan4 proxy disable false
admin@XorPlus# commit
```

set protocols arp inspection vlan disable

The **set protocols arp inspection vlan disable** command enables or disables ARP inspection in a VLAN.

Command Syntax

set protocols arp inspection vlan <*vlan-id*> **disable** <**true | false**>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
disable <**true	false**>	Enables or disables the ARP inspection. The value could be **true** or **false**. • **true**: disables the ARP inspection function. • **false**: enables the ARP inspection function. By default, ARP inspection function is disabled.

Usage Guidelines

When ARP inspection is enabled in a VLAN, the device checks ARP packets received on interfaces belong to the VLAN based on the static access lists (if configured) and the DHCP binding table except when the interface is a trust port (configured by using command **set protocols arp inspection trust-port** <*port-name*>).

NOTE:

Regardless of the fact that whether its static access lists or dynamic ARP inspection, you have to explicitly enable the ARP inspection function in the VLAN by using this command.

Example

- Enable ARP inspection in VLAN 100.

```
admin@XorPlus# admin@Xorplus# set protocols arp inspection vlan 100 disable false
admin@XorPlus# commit
```

set protocols arp inspection access-list ip mac-address

The **set protocols arp inspection access-list ip mac-address** command configures an ARP access list for ARP inspection.

NOTE:

When configuring the static access list for ARP Inspection, the same IP-MAC cannot exist in multiple access lists.

Command Syntax

set protocols arp inspection access-list <*acl-name*> **ip** <*ipv4-addr*> **mac-address** <*mac-addr*>

Parameters

Parameter	Description
access-list <*acl-name*>	Specifies access list name. The value is a string.
ip <*ipv4-addr*>	Specifies the IP address in a static ARP binding entry. The value is in dotted decimal notation.
mac-address <*mac-addr*>	Specifies the MAC address in a static ARP binding entry. The value is in the format H:H:H:H:H:H. An H contains 2 hexadecimal numbers. Note that, the MAC address cannot be configured to a multicast MAC or the system MAC.

Example

- Configure a static access list of ARP inspection that maps the IP address 10.0.0.1 to the MAC address 00:B0:BC:00:00:00.

```
admin@Xorplus# set protocols arp inspection access-list test1 ip 10.0.0.1 mac-address 00:B0:BC:00:00:00
admin@Xorplus# commit
```

set protocols arp inspection vlan access-list

The **set protocols arp inspection vlan access-list** command applies an ARP inspection access list to a VLAN.

Command Syntax

set protocols arp inspection vlan <*vlan-id*> **access-list** <*acl-name*>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
access-list <*acl-name*>	Specifies an access list name. The value is a string.

Usage Guidelines

A VLAN can be configured with multiple access-lists, and the system will check through the access-lists of the VLAN to match an ARP entry upon receiving an ARP packet. If no ARP entry is matched, the ARP packet will be dropped.

NOTE:

Configure the access-list first and then apply to a VLAN, otherwise it will prompt access-list does not exist when committing this command.

Example

- Apply the ARP inspection access list test1 to VLAN 100.

```
admin@Xorplus# set protocols arp inspection vlan 100 access-list test1
admin@Xorplus# commit
```

set protocols arp inspection trust-port

The **set protocols arp inspection trust-port** command configures an interface as a trust port on which ARP inspection will not be implemented.

Command Syntax

set protocols arp inspection trust-port <*port-name*>

Parameters

Parameter	Description
trust-port <*port-name*>	Specifies an interface name. The interface can be either a physical interface or an aggregated interface. By default, all interfaces are untrusted interfaces for ARP inspection.

Usage Guidelines

ARP inspection divides interfaces into trusted and untrusted ports. On trusted ports, the system does not perform ARP inspection on incoming ARP messages, allowing the ARP messages to pass. However, ARP inspection is required for ARP messages received on the untrusted port interface.

You can use the command **run show arp inspection interface** to show the trust state of all the interfaces for ARP inspection.

Example

- Configure the interface ge-1/1/1 as an ARP inspection trust port.

```
admin@Xorplus# set protocols arp inspection trust-port ge-1/1/1
admin@Xorplus# commit
```

run show arp

The **run show arp** command is used to view all IPv4 ARP entries.

Command Syntax

run show arp [**vrf** <*vrf-name*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string.

Usage Guidelines

When a VRF is specified, only the IPv4 ARP entries of the specific VRF are displayed.

When no VRF is specified, the result shows only the IPv4 ARP entries of the default VRF.

Example

- View all IPv4 ARP entries.

```
admin@Xorplus# run show arp
Aging-time(seconds): 1200
Total count        : 1
Address      HW Address       Type     Interface  Age
--------------  -----------------      -------     ----------   -----
20.20.20.3   70:72:CF:9D:6F:FB  Dynamic  vlan20    591
```

run show arp inspection dhcp-binding

The **run show arp inspection dhcp-binding** command displays the ARP inspection table. This table includes the ARP entries generated from the DHCP snooping or DHCP relay table.

Command Syntax

run show arp inspection dhcp-binding

Parameter

None.

Example

- Display the ARP inspection table.

```
admin@Xorplus# run show arp inspection dhcp-binding
Vlan  IP Address      Mac Address
----  --------------  -----------------
 2    100.1.1.1     14:18:77:18:2c:b9
```

run show arp inspection interface

The **run show arp inspection interface** command displays the trust state of all the interfaces for ARP inspection.

Command Syntax

run show arp inspection interface

Parameter

None.

Example

- Display the trust state of all the interfaces for ARP inspection.

```
admin@Xorplus# run show arp inspection interface
Interface   Trust State
----------  -----------
ge-1/1/1    Untrusted
ge-1/1/2    Trusted
...
ge-1/1/47   Untrusted
ge-1/1/48   Untrusted
te-1/1/1    Untrusted
te-1/1/2    Untrusted
```

Table 1 Description of the **run show arp inspection interface** command output

Item	Description
Interface	Indicates the interface name.
Trust State	Indicates the trust state of all the interfaces for ARP inspection. The value could be **Untrusted** or **Trusted**. The value is **Trusted** if the interface has been configured as trust port by using the command **set protocols arp inspection trust-port** <*port-name*>. Else, it prints **Untrusted**.

run show arp inspection vlan

The **run show arp inspection vlan** command displays ARP inspection configured information of a VLAN, such as, the configured static access lists of ARP inspection in the VLAN.

Command Syntax

run show arp inspection vlan <*vlan-id*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Display the configured static access lists of ARP inspection in VLAN 100.

```
admin@Xorplus# run show arp inspection vlan 100
Vlan  Configuration  Static ACL
----  -------------  ----------
100   Enabled        abc
                     bbb
```

Table 1 Description of the **run show arp inspection vlan** command output

Item	Description
Vlan	Indicates the VLAN ID.
Configuration	Indicates whether ARP inspection is enabled in the VLAN. The value could be **Enabled** or **Disabled**.
Static ACL	Indicates static access lists of ARP inspection in the VLAN if configured.

run show arp inspection access-list

The **run show arp inspection access-list** command displays the binding entries and applied VLANs of a static access list of ARP inspection.

Command Syntax

run show arp inspection access-list [*<acl-name>*]

Parameter

Parameter	Description
<acl-name>	Optional. Specifies access list name. The value is a string. If you do not specify an access list name, then display all configured access list; if an access list name is specified, then display configuration information of the specific access list.

Example

- Display the binding entries of the static access list test1 of ARP inspection.

```
admin@Xorplus# run show arp inspection access-list test1
Static ACL  IP Address       Mac Address
----------  ---------------  -----------------
Test1       1.1.22.1         00:00:00:00:00:11
            1.1.30.1         00:00:00:00:22:11
Static ACL  Applied Vlans
----------    -------------------
Test1       100  200  300  400
            500  600  700  800
            900  4000
```

- Display the binding entries of all the static access lists of ARP inspection.

```
admin@Xorplus# run show arp inspection access-list
Static ACL  IP Address       Mac Address
----------  ---------------  -----------------
abc         1.1.22.1         00:00:00:00:00:11
            1.1.30.1         00:00:00:00:22:11
bbb         1.1.11.1         00:00:00:22:22:11
```

Table 1 Description of the **run show arp inspection access-list** command output

Item	Description
Static ACL	Indicates the access list name.
IP Address	Indicates the IP address in a static ARP binding entry.
Mac Address	Indicates the MAC address in a static ARP binding entry.
Applied Vlans	Indicates the VLANs to which the static access list is applied to.

run show arp inspection statistics vlan

The **run show arp inspection statistics vlan** command displays the statistics of ARP inspection, such as, discarded and permitted ARP packets.

Command Syntax

run show arp inspection statistics vlan *<vlan-id>*

Parameter

Parameter	Description
vlan *<vlan-id>*	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.

Example

- Displays the statistics on discarded and permitted ARP packets by ARP inspection in VLAN 100.

```
admin@Xorplus# run show arp inspection statistics vlan 100
Vlan  Total Count  IP Validation Failures  MAC Validation Failures
----  -----------  ----------------------  -----------------------
100   10453        0                       0
Vlan  DHCP Drops  DHCP Permits  ACL Drops  ACL Permits
----  ----------  ------------  ---------  -----------
100   0           0             0          10453
```

Table 1 Description of the **run show arp inspection statistics vlan** command output

Item	Description
Vlan	Indicates the VLAN ID.
Total Count	Total number of the received ARP packets.
IP Validation Failures	Number of invalid IP addresses carried in incoming ARP messages, including multicast, broadcast and all 0 IP addresses.
MAC Validation Failures	Number of invalid MAC addresses carried in incoming ARP messages, including multicast MACs, broadcast MAC addresses, system MAC address, all 0 addresses and other invalid MAC addresses. Other invalid MAC addresses are ARP messages in which the source MAC address in the ARP message and the source MAC address in the Ethernet header are consistent.
DHCP Drops	Number of discarded ARP packets that matched no DHCP snooping binding entry.
DHCP Permits	Number of permitted ARP packets that matched the DHCP snooping binding entries.
ACL Drops	Number of discarded ARP packets that matched no entry of ARP inspection static access list.
ACL Permits	Number of permitted ARP packets that matched the entries of ARP inspection static access list.

protocols lacp interface <interface> priority

Users can set link aggregation option of gigabit-ethernet interface.

Command Syntax
set protocols lacp interface <*interface*> priority <*value*>
delete protocols lacp interface <*interface*> priority

Parameter
•<*interface*> Link aggregation option of gigabit-ethernet interface (e.g. ge-1/1/1)
•<*value*> Priority value, [0..65535]

Example
• This example is to set lacp priority of ge-1/1/1 to 3000 :

```
admin@XorPlus# set protocols lacp interface ge-1/1/1 priority 3000
admin@XorPlus# commit
```

protocols lacp priority

Users can configure the lacp priority of system.

Command Syntax
set protocols lacp priority <*value*>
delete protocols lacp priority

Parameter
•<*value*> Priority value, [0..65535]

Example
• This example is to set priorit of system to 1000:

```
admin@XorPlus# set protocols lacp priority 1000
admin@XorPlus# commit
```

protocols sflow agent-id

Users can set agent-id for sflow interface.

Command Syntax
set protocols sflow agent-id <*IPv4*>

Parameter
•<*IPv4*>A unique 32-bit identifier of the agent

Example
• This example is to set agent-id to 10.10.50.248:

```
admin@XorPlus# set protocols sflow agent-id 10.10.50.248
admin@XorPlus# commit
```

protocols sflow collector udp-port

Users can set sFlow collector IPv4 address.

Command Syntax
set protocols sflow collector <*IPv4*> udp-port <*port*>
delete protocols sflow collector <*IPv4*>

Parameter
•<*IPv4*> Configure the collector.
•<*port*> The UDP port of the collector, 6343 by default.

Usage Guidelines

To change the upd-port for a collector, you have to delete the collector configuration first and then set it back with the new upd-port.

For example,

Assume the original configuration as follows:

set protocols sflow collector 10.10.51.42 udp-port 3355

The following commands change the udp-port to 3366.

```
admin@Xorplus# delete protocols sflow collector 10.10.51.42
admin@Xorplus# commit
admin@Xorplus# set protocols sflow collector 10.10.51.42 udp-port 3366
admin@Xorplus# commit
```

Example
• This example is to configure the collector as 10.10.50.221,udp-port is 6343:

```
admin@XorPlus# set protocols sflow collector 10.10.50.221 udp-port 6343
admin@XorPlus# commit
```

protocols sflow disable

By default, sFlow is disabled. Users can enable sFlow and configure its' parameters.

Command Syntax
set protocols sflow disable <*bool*>
delete protocols sflow disable

Parameter
•<*bool*> Disable sflow on all interfaces by default

- **true** Disable sflow
- **false** enable sflow

Example
• This example is to enable sflow on all interface:

```
admin@XorPlus# set protocols sflow disable false
admin@XorPlus# commit
```

protocols sflow header-len

Users can set the length of sampled packet in bytes.

Command Syntax
set protocols sflow header-len <*len*>
delete protocols sflow header-len

Parameter
•<*len*>the Length of sampled packet in bytes

Example
• This example is to set length of sampled packet to 1024:

```
admin@XorPlus# set protocols sflow header-len 1024
admin@XorPlus# commit
```

protocols sflow interface <port> disable

Users can configure a specified interface to sflow protocol.

Command Syntax
set protocols sflow interface <*port*> disable <*bool*>
delete protocols sflow interface <*port*> disable

Parameter
•<*port*> ethernet switching port identifier,the valid ports range 1-52
•<*bool*>Disable or enable sflow on a specified interface

- **true** Disable sflow on a specified interface
- **false** enable sflow on a specified interface

Example
• This example is to enable sflow on ge-1/1/3:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 disable false
admin@XorPlus# commit
```

protocols sflow interface <port> header-len

Users can set the Length of sampled packet in bytes.

Command Syntax
set protocols sflow interface <*port*> header-len <*value*>
delete protocols sflow interface <*port*> header-len

Parameter
•<*port*> ethernet switching port identifier,the valid ports range 1-52
•<*value*> The length identifier, [14..9216]

Example
• This example is to set header length sampled packets to 15 on ge-1/1/3:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 header-len 15
admin@XorPlus#
```

protocols sflow interface <port> polling-interval

Users can set the polling interval for a specified interface.

Command Syntax
set protocols sflow interface <*port*> polling-interval <*seconds*>
*d*elete protocols sflow interface <*port*> polling-interval

Parameter
•<*port*> ethernet switching port identifier,the valid ports range 1-52
•<*seconds*> Number of seconds, [0..3600]

Example
• This example is to set polling interval to 300 on ge-1/1/3:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 polling-interval 300
admin@XorPlus# commit
```

protocols sflow interface <port> sampling-rate egress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow interface <*port*> sampling-rate egress <*value*>
delete protocols sflow interface <*port*> sampling-rate egress

Parameter
•<*value*>the rate at which exiting packets must be sampled, 2000 by default,[0..1048576]

Example
• This example is to set sampling rate of egress to 1000:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 sampling-rate egress 1000
admin@XorPlus# commit
```

protocols sflow interface <port> sampling-rate ingress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow interface <*port*> sampling-rate ingress <*value*>
delete protocols sflow interface <*port*> sampling-rate ingress

Parameter
•<*value*>the rate at which exiting packets must be sampled, 2000 by default,[0..1048576]

Example
• This example is to set sampling rate of ingress to 1000:

```
admin@XorPlus# set protocols sflow interface ge-1/1/3 sampling-rate ingress 1000
admin@XorPlus# commit
```

protocols sflow polling-interval

Users can set polling interval the sflow agent polls interfaces in seconds.

Command Syntax
set protocols sflow polling-interval <*time*>

Parameter
•<*time*> Number of seconds, how often the sflow agent polls interfaces in seconds, 30 by default

Example
• This example is to set polling interval to 60:

```
admin@XorPlus# set protocols sflow polling-interval 60
admin@XorPlus# commit
```

protocols sflow sampling-rate egress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow sampling-rate egress <*value*>
delete protocols sflow sampling-rate egress

Parameter
•<*value*>the rate at which exiting packets must be sampled, 2000 by default,[0..1048576]

Example
• This example is to set sampling rate of egress to 1000:

```
admin@XorPlus# set protocols sflow sampling-rate egress 1000
admin@XorPlus# commit
```

protocols sflow sampling-rate ingress

Users can set the sampling rate of sflow agent.

Command Syntax
set protocols sflow sampling-rate ingress <*value*>
delete protocols sflow sampling-rate ingress

Parameter
•<*value*>the rate at which exiting packets must be sampled, 2000 by default,[0..1048576]

Example
• This example is to set sampling rate of ingress to 1000:

```
admin@XorPlus# set protocols sflow sampling-rate ingress 1000
admin@XorPlus# commit
```

protocols sflow source-address

Users can set the source address as the source in packets transmitted to collectors.

Command Syntax
set protocols sflow source-address <*IPv4*>

Parameter
•<*IPv4*>source address as the source in packets transmitted to collectors

Example
• This example is to set source-address to 10.10.50.248:

```
admin@XorPlus# set protocols sflow source-address 10.10.50.248
admin@XorPlus# commit
```

set protocols dhcp snooping vlan

The **set protocols dhcp snooping vlan disable** command enables DHCP snooping in a specified VLAN.

Command Syntax

set protocols dhcp snooping vlan <*vlan-id*> **disable** <**true** | **false**>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
disable <**true**	**false**>	Enables or disables DHCP snooping, the value could be **true** or **false**: • **true**: Disables DHCP snooping. • **false**: Enables DHCP snooping. By default, DHCP snooping is disabled.

Usage Guidelines

DHCP snooping should be enabled in the VLAN, it takes effect only on the DHCP messages received from the VLAN enabled with DHCP snooping function. Packets received from the VLANs with DHCP snooping disabled will not be processed by the DHCP snooping module, and they will be processed and forwarded by the device as ordinary packets.

NOTE:

- The DHCP snooping function is only practicable to the clients directly connected to the local L2 domain, rather than connected through a router.
- When DHCP snooping is disabled, the DHCP binding entry for the VLAN will be removed correspondingly.

Example

- Enable DHCP snooping in VLAN 12.

```
admin@Xorplus# set protocols dhcp snooping vlan 12 disable false
```

set protocols dhcp snooping trust-port

The **set protocols dhcp snooping trust-port** command configures an interface as a trust interface for DHCP snooping.

Command Syntax

set protocols dhcp snooping trust-port <*interface-name*>

Parameters

Parameter	Description
trust-port <*interface-name*>	Specifies an interface name. The interface can be either a physical interface or an aggregated interface. By default, all interfaces are untrusted interfaces.

Usage Guidelines

In order to make the DHCP client obtain an IP address from a legitimate DHCP server, the device interface directly or indirectly connected to the DHCP server trusted by the administrator must be set to the trust interface, so as to prevent a spoofing DHCP server from assigning an IP address to the DHCP client.

The trusted interface forwards DHCP packets received from the DHCP server normally, whereas the untrusted interface discards DHCP ACK and DHCP OFFER packets received from the DHCP server.

Example

- Configure ge-1/1/1 as trust port for DHCP snooping.

```
admin@Xorplus# set protocols dhcp snooping trust-port ge-/1/1/1
```

set protocols dhcp snooping vlan option82-policy

The **set protocols dhcp snooping vlan option82-policy** command configures how to handle the Option 82 field when receiving a DHCP Discover/Request/Release/Decline/Inform message with Option 82 on VLANs where DHCP snooping is enabled.

Command Syntax

set protocols dhcp snooping vlan <*vlan-id*> **option82-policy <drop | keep | insert | replace>**

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
option82-policy <**drop	keep	insert	replace>**	Specifies the policy for Option 82. The value could be **drop**, **keep**, **insert** or **replace**. • **drop**: drop the packet if have Option 82. If the received DHCP packets have no Option 82 values, the packets will be forwarded. • **keep**: Option 82 in the packet remains unchanged and forwarded. • **insert**: the existing Option 82 sub-options remain unchanged, and the non-existing Option 82 sub-options will be inserted with the value the administrator configured, then forward the packet to the DHCP server. • **replace**: The non-existing Option 82 sub-options, will be inserted with the value the administrator configured. The existing Option 82 sub-options will be replaced with the value administrator configured, and then forward the packet. The default value is **keep**.

Usage Guidelines

Option 82 policy is used when receiving a DHCP Discover/Request/Release/Decline/Inform message from the DHCP client. When option82-policy is set to “insert” or “replace”, you can use the following commands to set the format of circuit ID and remote ID sub-options:

set protocols dhcp snooping option82 circuit-id <**port-index | port-name | port-description**>

set protocols dhcp snooping option82 remote-id <**system-mac | hostname**>

We can use the following table to summarize the Option 82 policy.

Received Packet / Option82 Policy	No Option82	Only Circle ID	Only Remote ID	Circle ID + Remote ID
drop	The packet is forwarded without changing option 82.	The packet is dropped.	The packet is dropped.	The packet is dropped.
keep	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.
insert	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: unchanged. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: unchanged.	The packet is forwarded. Circle ID: unchanged. Remote ID: unchanged.
replace	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: replaced with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: replaced with the value configured.

For details about how Option 82 is processed by the DHCP snooping and DHCP relay module, see Introduction to DHCP.

Example

- Configure the Option 82 policy.

```
admin@Xorplus# set protocols dhcp snooping vlan 12 option82-policy insert
```

set protocols dhcp snooping option82 circuit-id

The **set protocols dhcp snooping option82 circuit-id** command configures the format of sub-option circuit ID inserted into the Option 82 field for DHCP snooping.

NOTE: The sub-option circuit ID is applied to VLANs where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp snooping option82 circuit-id <**port-index** | **port-name** | **port-description**>

Parameters

Parameter	Description
circuit-id <**port-index	port-name	port-description**>	Specifies the type of circuit ID in the Option 82 field. The value could be **port-index**, **port-name** or **port-description**. By default, the sub-option circuit ID is not configured which means circuit ID is not enabled.

Usage Guidelines

If configured, the circuit ID is filled with the port identifier and VLAN.

- When “port-index” is selected, the format of the circuit ID is “VLAN ID + port index”.
- When “port-name” is selected, the format of the circuit ID is “VLAN ID + port name”.
- When “port-description” is selected, the format of the circuit ID is “VLAN ID + port description”. The value of “port-description” can be set by the following commands:

set interface aggregate-ethernet <*lag_name*> **description** <*description*>

set interface gigabit-ethernet <*physical-port*> **description** <*description*>

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the format of the sub-option circuit ID for the Option 82 field.

```
admin@Xorplus# set protocols dhcp snooping option82 circuit-id port-index
```

set protocols dhcp snooping option82 remote-id

The **set protocols dhcp snooping option82 remote-id** command configures the format of sub-option remote ID inserted into the DHCP Option 82 field for DHCP snooping.

NOTE: The sub-option remote ID is applied to VLANs where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp snooping option82 remote-id <**system-mac** | **hostname**>

Parameters

Parameter	Description
remote-id <system-mac | hostname>	Specifies the type of remote ID in the Option 82 field. The value could be **system-mac** or **hostname**. By default, the sub-option remote ID is not configured which means remote ID is not enabled.

Usage Guidelines

If configured, the remote ID is unique per switch.

- When “system-mac” is selected, the format of the remote ID is “system MAC”.
- When “hostname” is selected, the format of the remote ID is “hostname”. The value of “hostname” can be set by the following command:

set system hostname <*hostname*>

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the type of sub-option remote ID inserted into the DHCP Option 82 field.

```
admin@Xorplus# set protocols dhcp snooping option82 remote-id system-mac
```

set protocols dhcp snooping option82 trust-all

The **set protocols dhcp snooping option82 trust-all** command is used to enable or disable Option 82 trust-all function for DHCP snooping.

Command Syntax

set protocols dhcp snooping option82 trust-all <**true | false**>

Parameters

Parameter	Description
<**true** | **false**>	Enables or disables Option 82 trust-all function, the value could be **true** or **false**: • **true**: Enables Option 82 trust-all function. • **false**: Disables Option 82 trust-all function. By default, Option 82 trust-all function is disabled.

Usage Guidelines

DHCP Discover/Request/Release/Decline/Inform packets received on the switch without giaddr but containing Option 82 are dropped by default. To allow these packets on the switch, PICOS supports Option 82 trust all function:

- If trust all is enabled, such packets will be processed according to the configuration of the Option 82 policy.
- If trust all is disabled, then drop the packets.

This command is useful if there is a switch in between the client and the DHCP snooping device that may insert Option 82. Use this command to ensure that these packets do not get dropped.

Example

- Enable Option 82 trust-all function.

```
admin@Xorplus# set protocols dhcp snooping option82 trust-all true
```

set protocols dhcp snooping binding file

The **set protocols dhcp snooping binding file** command configures a DHCP snooping binding file for synchronizing DHCP snooping entries from memory.

Command Syntax

set protocols dhcp snooping binding file *<file-path>*

Parameters

Parameter	Description
file *<file-path>*	Specifies a file path to save the DHCP snooping binding table.

Usage Guidelines

If a DHCP snooping binding file is specified, the DHCP snooping entries will be synchronized from the memory to the binding file. This prevents DHCP snooping entries data loss in case of power failure. By setting a DHCP snooping binding file, the system can directly load the existing snooping entries from the binding file after if recovers.

Example

- Configure the DHCP snooping binding file.

```
admin@Xorplus# set protocols dhcp snooping binding file /tmp/run/dhcp_bind
admin@XorPlus# commit
```

set protocols dhcp snooping binding write-delay

The **set protocols dhcp snooping binding write-delay** command configures a delay timer for writing the DHCP snooping entries from memory to the binding file.

Command Syntax

set protocols dhcp snooping binding write-delay <*write-delay-timer*>

Parameters

Parameter	Description
write-delay <*write-delay-timer*>	Specifies a delay timer for writing the DHCP snooping entries from the memory to the binding file. The value is an integer in seconds that ranges from 15 to 86400. The default value is 300s.

Usage Guidelines

In order to reduce the system burden caused by frequent file writes, you can configure a delay timer for writing the DHCP snooping entries from memory to the binding file.

NOTE:

In the case when the DHCP snooping entry is changed by the administrator configuration modifications from the CLI, such as modifying the VLAN, the binding file will be immediately refreshed rather than wait for write-delay timer.

Example

- Configure a delay timer for writing the DHCP snooping entries from memory to the binding file.

```
admin@Xorplus# set protocols dhcp snooping binding write-delay 24
admin@XorPlus# commit
```

run show dhcp snooping binding

The **run show dhcp snooping binding** command displays the DHCP snooping binding table, which includes the user MAC address, IP address, VLAN ID, access interface and the lease time.

Command Syntax

run show dhcp snooping binding

Parameter

None.

Example

- Show the DHCP snooping binding table.

```
admin@Xorplus# run show dhcp snooping binding
Total count:     2
MAC Address         IP Address     Port            VLAN ID   Lease(sec)
-------------------------------------------------------------------------------------------
e4:f0:04:89:b6:46   0.0.0.0         ae65            1         0/0
14:18:77:18:2c:b9   100.1.1.1       ae25            125       599/600
```

Table 1. Description of the run show dhcp snooping binding command output

Item	Description
Mac Address	User MAC address.
IP Address	User IP address.
Port	User access interface.
VLAN ID	User VLAN ID.
Lease(sec)	Lease time for the IP address, in seconds. The format displayed is **Remaining Lease Time/Total Lease Time**.

set protocols dhcp relay interface disable

The **set protocols dhcp relay interface disable** command enables or disables DHCP relay on a specified L3 interface.

Command Syntax

set protocols dhcp relay interface <*l3-interface-name*> **disable <true | false>**

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
disable <**true** | **false**>	Enables or disables DHCP relay on an L3 interface, the value could be **true** or **false**: • **true**: Disables DHCP relay. • **false**: Enables DHCP relay. By default, DHCP relay is disabled.

Usage Guidelines

Generally, DHCP relay should be enabled on the L3 interface that connects to the host's network.

Example

- Enable DHCP relay on the L3 VLAN interface vlan100.

```
admin@Switch# set protocols dhcp relay interface vlan100 disable false
```

set protocols dhcp relay interface dhcp-server-address

The **set protocols dhcp relay interface dhcp-server-address** command configures a DHCP server address on the L3 interface enabled with DHCP relay.

Command Syntax

set protocols dhcp relay interface <*l3-interface-name*> **dhcp-server-address** <*server-ipv4-address*>

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
dhcp-server-address <*server-ipv4-address*>	Specifies the IPv4 address of a DHCP server. The value is in dotted decimal notation.

Usage Guidelines

You can repeat this command to configure multiple DHCP servers.

NOTE: The DHCP server IP address should not be in the same subnet with the L3 interface enabled with the DHCP relay.

Example

- Configure DHCP relay and DHCP server address on L3 VLAN interface vlan100.

```
admin@Xorplus# set protocols dhcp relay interface vlan100 dhcp-server-address 10.10.1.1
```

set protocols dhcp relay interface relay-agent-address

The **set protocols dhcp relay interface relay-agent-address** command configures the IP address of the DHCP relay agent.

Command Syntax

set protocols dhcp relay interface <*l3-interface-name*> **relay-agent-address** <*agent-ipv4-address*>

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
relay-agent-address <*agent-ipv4-address*>	Specifies the IP address of the DHCP relay agent. The value is in dotted decimal notation.

Usage Guidelines

DHCP relay agent address is a required configuration in VRRP topology, when the VRRP Master/Backup devices are used as the DHCP relay agents, you must configure the DHCP relay agent address to the virtual IP address of the VRRP group.

The interface name here should be configured with the L3 interface which is enabled with DHCP relay and VRRP group.

However, in a non-VRRP topology, there's no need to configure the DHCP relay agent address. By default, the system sets the IP address of the L3 interface that is enabled with the DHCP relay as the DHCP relay agent address.

The system supports multiple DHCP relay agent addresses on a switch, one DHCP relay agent address for each VRRP group.

Example

- Con*figure a DHCP relay agent address* on L3 VLAN interface vlan100.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 1 ip 192.168.1.5
admin@Xorplus# set protocols dhcp relay interface vlan100 relay-agent-address 192.168.1.5
```

set protocols dhcp relay interface option82-policy

The **set protocols dhcp relay interface option82-policy** command configures how to handle the Option 82 field when receiving a DHCP Discover, DHCP Request, DHCP Release, DHCP Decline or DHCP Inform message with Option 82 on the L3 interfaces where DHCP relay is enabled.

Command Syntax

set protocols dhcp relay interface <*l3-interface-name*> **option82-policy <drop | keep | insert | replace>**

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
option82-policy <**drop	keep	insert	replace**>	Specifies the policy for Option 82. The value could be **drop**, **keep**, **insert** or **replace**. • **drop**: drop the packet if have Option 82. If the received DHCP packets have no Option 82 values, the packets will be forwarded. • **keep**: Option 82 in the packet remains unchanged and forwarded. • **insert**: the existing Option 82 sub-options remain unchanged, and the non-existing Option 82 sub-options will be inserted with the value the administrator configured, then forward the packet to the DHCP server. • **replace**: The non-existing Option 82 sub-options, will be inserted with the value the administrator configured. The existing Option 82 sub-options will be replaced with the value administrator configured, and then forward the packet. The default value is **keep**.

Usage Guidelines

Option 82 policy is used when receiving a DHCP Discover/Request/Release/Decline/Inform message from the DHCP client. When option82-policy is set to “insert” or “replace”, you can use the following commands to set the format of sub-option circuit ID and remote ID:

set protocols dhcp relay option82 circuit-id <port-index | port-name | port-description>

set protocols dhcp relay option82 remote-id <system-mac | hostname>

We can use the following table to summarize the Option 82 policy.

Received Packet / Option82 Policy	No Option82	Only Circle ID	Only Remote ID	Circle ID + Remote ID
drop	The packet is forwarded without changing option 82.	The packet is dropped.	The packet is dropped.	The packet is dropped.
keep	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.	The packet remains unchanged and forwarded.
insert	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: unchanged. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: unchanged.	The packet is forwarded. Circle ID: unchanged. Remote ID: unchanged.
replace	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: inserted with the value configured.	The packet is forwarded. Circle ID: inserted with the value configured. Remote ID: replaced with the value configured.	The packet is forwarded. Circle ID: replaced with the value configured. Remote ID: replaced with the value configured.

For details about how Option 82 is processed by the DHCP snooping and DHCP relay module, see Introduction to DHCP.

Example

- Configure the Option 82 policy.

```
admin@Xorplus# set protocols dhcp relay interface vlan12 option82-policy insert
```

set protocols dhcp relay option82 circuit-id

The **set protocols dhcp relay option82 circuit-id** command configures the format of sub-option circuit ID inserted into the DHCP Option 82 field for DHCP relay.

NOTE: The sub-option circuit ID is applied to VLAN interfaces where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp relay option82 circuit-id <**port-index** | **port-name** | **port-description**>

Parameters

Parameter	Description
circuit-id <port-index | port-name | port-description>	Specifies the format of circuit ID in the Option 82 field. The value could be **port-index**, **port-name** or **port-description**. By default, the sub-option circuit ID is not configured, which means circuit ID is not enabled.

Usage Guidelines

If configured, the circuit ID is filled with port identifier and VLAN:

- When “port-index” is selected, the format of the circuit ID is “VLAN ID + port index”.
- When “port-name” is selected, the format of the circuit ID is “VLAN ID + port name”.
- When “port-description” is selected, the format of the circuit ID is “VLAN ID + port description”. The value of “port-description” can be set by the following commands:

set interface aggregate-ethernett <*lag_name*> **description** <*description*>

set interface gigabit-ethernet <*physical-port-name*> **description** <*description*>

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the format of sub-option circuit ID in the Option 82 field to port-index.

```
admin@Xorplus# set protocols dhcp relay option82 circuit-id port-index
```

set protocols dhcp relay option82 remote-id

The **set protocols dhcp relay option82 remote-id** command configures the format of sub-option remote ID inserted into the DHCP Option 82 field for DHCP relay.

NOTE: The sub-option remote ID is applied to VLAN interfaces where option82-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp relay option82 remote-id <**system-mac** | **hostname**>

Parameters

Parameter	Description
remote-id <system-mac | hostname>	Specifies the format of remote ID in the Option 82 field. The value could be **system-mac** or **hostname**. By default, the sub-option remote ID is not configured, which means remote ID is not enabled.

Usage Guidelines

If configured, the remote ID is unique per switch.

- When “system-mac” is selected, the format of the remote ID is “system MAC”.
- When “hostname” is selected, the format of the remote ID is “hostname”. The value of “hostname” can be set by the system hostname command:

set system hostname <*hostname*>

Note that, when configuring Option 82 in MLAG environment, remote ID should be set to “system-mac” and circuit ID should be set to “port-index”.

Example

- Configure the format of sub-option remote ID inserted into the DHCP Option 82 field.

```
admin@Xorplus# set protocols dhcp relay option82 remote-id system-mac
```

set protocols dhcp relay option82 trust-all

The **set protocols dhcp relay option82 trust-all** command is used to enable or disable Option 82 trust-all function for DHCP relay.

Command Syntax

set protocols dhcp relay option82 trust-all <**true | false**>

Parameters

Parameter	Description
<**true** | **false**>	Enables or disables Option 82 trust-all function, the value could be **true** or **false**: • **true**: Enables Option 82 trust-all function. • **false**: Disables Option 82 trust-all function. By default, Option 82 trust-all function is disabled.

Usage Guidelines

DHCP Discover/Request/Release/Decline/Inform packets received on the switch without giaddr but containing Option 82 are dropped by default. To allow these packets on the switch, PICOS supports Option 82 trust all function:

- If trust all is enabled, such packets will be processed according to the configuration of the Option 82 policy.
- If trust all is disabled, then drop the packets.

This command is useful if there is a switch in between the client and the relay agent that may insert Option 82. Use this command to ensure that these packets do not get dropped.

Example

- Enable Option 82 trust-all function.

```
admin@Xorplus# set protocols dhcp relay option82 trust-all true
```

set protocols dhcp server pool network

The **set protocols dhcp server pool network** command creates an IPv4 address pool and the network that can be assigned to the DHCP clients.

Command Syntax

set protocols dhcp server pool <*pool-name*> **network** <*IPv4Net*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
network <*IPv4Net*>	Specify an IPv4 network segment from which DHCP server can dynamically assign IP addresses to the DHCP clients. The value is in the form of *IPv4_address/ prefix_length*, where *prefix_length* can range from 1 to 32. For example, 10.10.10.0/24.

Usage Guidelines

The DHCP server can assign IP addresses to the DHCP clients from the configured address pool.

NOTE:

- Each address pool can be configured with only one network segment. If the system needs multiple segments, multiple address pools need to be configured, but there can be no address overlap between pools.
- The network segment of the address pool should be the same network segment as the IP of the VLAN interface connected to the client.

Example

- Create an IPv4 address pool pool1, and the network is 10.1.10.0/24.

```
admin@Xorplus# set protocols dhcp server pool pool1 network 10.1.10.0/24
admin@Xorplus# commit
```

set protocols dhcp server pool range low

The **set protocols dhcp server pool range low** command configures the lower boundary of a range of addresses in the address pool.

Command Syntax

set protocols dhcp server pool <*pool-name*> **range** <*range-name*> **low** <*ipv4-address*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
range <*range-name*>	Specifies a range name of addresses. The value is a string of case-sensitive characters, spaces are not supported.
low <*ipv4-address*>	Specifies the lower boundary of a range of addresses. The value is in dotted decimal notation.

Usage Guidelines

This command should be configured together with the command **set protocols dhcp server pool** <*pool-name*> **range** <*range-name*> **high** <*ipv4-address*>, separately configuring the lower and upper boundaries of an address range of an address pool. The address range is required to be a subnet of the address pool.

NOTE:

- The address range is optional. If not configured, it means that all the IP addresses in the address pool are available for address assignment. However, if configured, only addresses in the range are used for address assignment.
- When multiple address ranges are configured under an address pool, there should be no address overlap between different ranges.

Example

- Configure a range of addresses.

```
admin@Xorplus# set protocols dhcp server pool pool1 range range1 low 10.1.10.2
admin@Xorplus# set protocols dhcp server pool pool1 range range1 high 10.1.10.225
admin@Xorplus# commit
```

set protocols dhcp server pool range high

The **set protocols dhcp server pool range high** command configures the upper boundary of a range of addresses in the address pool.

Command Syntax

set protocols dhcp server pool <*pool-name*> **range** <*range-name*> **high** <*ipv4-address*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
range <*range-name*>	Specifies a range name of addresses. The value is a string of case-sensitive characters, spaces are not supported.
high <*ipv4-address*>	Specifies the upper boundary of a range of addresses. The value is in dotted decimal notation.

Usage Guidelines

This command should be configured together with the command **set protocols dhcp server pool** <*pool-name*> **range** <*range-name*> **low** <*ipv4-address*>, separately configuring the lower and upper boundaries of an address range of an address pool. The address range is required to be a subnet of the address pool.

NOTE:

- The address range is optional. If not configured, it means that all the IP addresses in the address pool are available for address assignment. However, if configured, only addresses in the range are used for address assignment.
- When multiple address ranges are configure under an address pool, there should be no address overlap between different ranges.

Example

- Configure a range of addresses.

```
admin@Xorplus# set protocols dhcp server pool pool1 range range1 low 10.1.10.2
admin@Xorplus# set protocols dhcp server pool pool1 range range1 high 10.1.10.225
admin@Xorplus# commit
```

set protocols dhcp server pool domain-name

The **set protocols dhcp server pool domain-name** command configures a DNS domain name assigned to a DHCP client.

Command Syntax

set protocols dhcp server pool <*pool-name*> **domain-name** <*domain-name*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
domain-name <*domain-name*>	Specifies a domain name to be assigned to a DHCP client. The value is a string of 1 to 128 characters without spaces.

Usage Guidelines

On the DHCP server, use the command **set protocols dhcp server pool** <*pool-name*> **domain-name** <*domain-name*> to specify the domain name suffix to assign to the DHCP client for each address pool. The DHCP server sends the domain name to the client when allocating IP address to the client.

Example

- Configure a DNS domain name.

```
admin@Xorplus# set protocols dhcp server pool pool1 domain-name company.com
admin@Xorplus# commit
```

set protocols dhcp server pool dns-server

The **set protocols dhcp server pool dns-server** command configures a DNS server address for an address pool.

Command Syntax

run show vrf

set protocols dhcp server pool <*pool-name*> **dns-server** <*dns-server-ip*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
dns-server <*dns-server-ip*>	Specifies the DNS server address. The value is in dotted decimal notation.

Usage Guidelines

DNS servers are used for domain name resolution. To enable DHCP clients to communicate with devices on other networks through host names, configure the DNS server.

To enable DNS services for the DHCP client, specify the DNS server address for the address pool on the DHCP server. When allocating IP address to the client, the DHCP server sends the DNS server address to the client.

Repeatedly configure this command to configure multiple DNS servers. Each address pool can be configured with a maximum of eight DNS server addresses.

Example

- Configure a DNS server address for an address pool.

```
admin@Xorplus# set protocols dhcp server pool pool1 dns-server 10.3.10.1
admin@Xorplus# commit
```

set protocols dhcp server pool default-router

The **set protocols dhcp server pool default-router** command configures a default gateway address for the DHCP clients.

Command Syntax

set protocols dhcp server pool <*pool-name*> **default-router** <*router-ip address*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
default-router <*router-ip address*>	Specifies an egress gateway address. The value is in dotted decimal notation.

Usage Guidelines

In order to allow the DHCP client to access the network normally, the default gateway can be configured for the DHCP clients to send and receive user data.

Example

- Configure a default gateway address for the DHCP clients.

```
admin@Xorplus# set protocols dhcp server pool pool1 default-router 10.10.10.1
admin@Xorplus# commit
```

set protocols dhcp server pool lease-time

The **set protocols dhcp server pool lease-time** command configures the lease time for IP addresses in an address pool.

Command Syntax

set protocols dhcp server pool <*pool-name*> **lease-time** <*lease-time*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
lease-time <*lease-time*>	Specifies the lease time for IP addresses. The value is an integer that ranges from 2 to 4294967295, in minute. The default value is 60 minutes.

Example

- Configure the lease for IP addresses in an address pool to two days.

```
admin@Xorplus# set protocols dhcp server pool pool2 lease-time 2880
admin@Xorplus# commit
```

set protocols dhcp server pool vrf

The **set protocols dhcp server pool vrf** command assigns a DHCP address pool to a VRF.

Command Syntax

set protocols dhcp server pool <*pool-name*> **vrf** <*vrf-name*>

Parameter

Parameter	Description
pool <*pool-name*>	Specifies an address pool name. The value is a string of case-sensitive characters, spaces are not supported.
vrf <*vrf-name*>	Specifies a VRF name. The value is a string of case-sensitive characters, spaces are not supported.

Usage Guidelines

In most cases, one address pool allocates IP addresses to clients in only one network segment to prevent IP address conflicts. However, in VRF scenario, different VRFs can use IP addresses on the same network segment. This command can be used to assign different DHCP address pools to different VRFs.

To enable the IP address allocation on the same network segment in two different VRFs, first you have to configure two different pools with the same network segment, and then assign the DHCP address pools to different VRFs separately.

NOTE:

- If a pool is not associated with any specific VRF, by default, it is assigned to the default VRF.
- Each pool can only be assigned to one VRF, but each VRF can be associated to multiple pools.
- DHCP server supports VRF by binding the address pool and the VLAN interface (which is connected to the DHCP client) to the same VRF.

Example

- Assign a DHCP address pool to a VRF.

```
admin@Xorplus# set protocols dhcp server pool pool2 vrf vrf1
admin@Xorplus# commit
```

run show dhcp server binding address

The **run show dhcp server binding address** command shows the allocated IP address binding information.

Command Syntax

run show dhcp server binding [**vrf** <*vrf-name*>] [**address <***ipv4-address***>**]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>]. Note that: The command shows the allocated IP address binding information in the default VRF if not explicitly specify a VRF name.
address <*ipv4-address***>**	Optional. Specifies an allocated address. The value is in dotted decimal notation.

Example

- View the allocated IP address binding information.

```
admin@Xorplus# run show dhcp server binding
2 bound clients

IP address      MAC address          Server      Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1    vlan100
10.1.1.88       00:0a:12:00:12:34    10.1.1.1    vlan100

admin@Xorplus# run show dhcp server binding vrf vrf1
1 bound clients

IP address      MAC address          Server     Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1   vlan100

admin@Xorplus# run show dhcp server binding address 10.1.1.89
IP address      MAC address          Server     Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1   vlan100

admin@Xorplus# run show dhcp server binding vrf vrf1 address 10.1.1.89
IP address      MAC address          Server     Interface
10.1.1.89       00:0a:12:00:12:12    10.1.1.1   vlan100
```

In the show result, "**Server**" represents the IP address of the Layer 3 VLAN interface connected to the DHCP client.

run show dhcp server binding interface

The **run show dhcp server binding interface** command displays the allocated IP address binding information based on the VLAN interface and configuration information of other parameters, including DNS server, domain name and default router.

Command Syntax

run show dhcp server binding interface {**all |** <*interface-name*>}

Parameter

Parameter	Description
interface {**all |** <*interface-name*>}	Specifies an L3 VLAN interface name. The value could be **all** or a specific VLAN interface name, where **all** indicates to show DHCP client information of all the VLAN interfaces.

Example

- View the allocated IP address binding information based on the VLAN interface.

```
admin@Xorplus# run show dhcp server binding interface vlan100
2 bound clients

Client Interface: vlan100

    MAC address:          00:0a:12:00:12:11
    Client IP Address:      10.1.1.88

    MAC address:          00:0a:12:00:12:12
    Client IP Address:      10.1.1.89

    DHCP Options :
    Name: dhcp-lease-time, Value: 43200 minutes
    Name: name-server, Value: [ 10.209.194.131, 198.51.110.2, 192.0.2.3 ]
    Name: server-identifier, Value: 10.1.1.1
    Name: router, Value: [ 10.1.1.1 ]
    Name: domain-name, Value: example-50
```

Table 1. Description of the run show dhcp server binding interface command output

Item	Description
MAC address	Indicates the MAC address of a DHCP client.
Client IP Address	Indicates the IP address of a DHCP client.
Name: dhcp-lease-time	Indicates the lease time of the IP addresses.
Name: name-server	Indicates the IP address of the DNS server.
Name: server-identifier	Indicates the IP address of Layer 3 VLAN interface connected to the DHCP client.
Name: router	Indicates the default gateway for the DHCP clients.
Name: domain-name	Indicates the domain name for the DHCP clients.

set protocols dhcp6 relay interface disable

The **set protocols dhcp6 relay interface disable** command enables or disables DHCPv6 relay on a specified L3 interface.

Command Syntax

set protocols dhcp6 relay interface <*l3-interface-name*> **disable <true | false>**

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
disable <**true** | **false**>	Enables or disables DHCPv6 relay on an L3 interface, the value could be **true** or **false**: • **true**: Disables DHCPv6 relay. • **false**: Enables DHCPv6 relay. By default, DHCPv6 relay is disabled.

Usage Guidelines

Generally, DHCPv6 relay should be enabled on the L3 interface that connects to the host's network.

Example

- Enable DHCPv6 relay on the L3 VLAN interface vlan100.

```
admin@Switch# set protocols dhcp6 relay interface vlan100 disable false
```

set protocols dhcp6 relay interface destination

The **set protocols dhcp6 relay interface destination** command configures the IPv6 address of the DHCPv6 server or next-hop relay agent on the L3 interface enabled with DHCPv6 relay. You can repeat this command to configure multiple DHCPv6 servers.

Command Syntax

set protocols dhcp6 relay interface <*l3-interface-name*> **destination** <*ipv6-address*>

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name.
destination <*ipv6-address*>	Specifies the destination address of relay messages, which can be the IPv6 address of the DHCPv6 server or next hop relay agent. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Example

- Configure the IPv6 address of the DHCPv6 server or next-hop relay agent on interface vlan100.

```
admin@Xorplus# set protocols dhcp6 relay interface vlan100 destination 205:147::205
```

set protocols dhcp6 relay interface remote-id

The **set protocols dhcp6 relay interface remote-id** command configures the remote ID to be inserted into the DHCPv6 relay packets.

Command Syntax

set protocols dhcp6 relay interface <*l3-interface-name*> **remote-id** <*remote-id*>

Parameters

Parameter	Description
interface <*l3-interface-name*>	Specifies an L3 interface name. The value could be the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. Its the outbound interface of relay messages.
remote-id <*remote-id*>	Specifies the remote ID. The value is a string.

Usage Guidelines

The Remote ID records user access information in the DHCPv6 packets sent from the clients to the device. When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the DHCPv6 relay can insert the Remote ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters.

Example

- Configure the remote ID to be inserted into the DHCPv6 relay packets.

```
admin@Xorplus# set protocols dhcp6 relay interface vlan100 remote-id ubuntuDesktop16.04.6-2
```

run show dhcp6 relay-stats

The **run show dhcp6 relay-stats** command displays DHCPv6 relay running status and statistics.

Command Syntax

run show dhcp6 relay-stats

Parameter

None.

Example

- Display DHCPv6 relay running status and statistics.

```
admin@Xorplus# run show dhcp6 relay-stats
Vif Name        Rx        Tx
-----------------------------------
vlan10          6866      1626
vlan20          2455      896
Total 2 Vif(s) enabled with DHCP6 relay
```

set protocols lacp interface rate

The **set protocols lacp interface rate** command configures the fast rate at which the peer switch interface sends LACP PDUs.

Command Syntax

set protocols lacp interface <*interface-name*> **rate** <**fast | slow** >

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name of the switch.
rate <**fast	slow** >	Specifies the rate at which the peer switch interface sends LACP PDUs. The value could be **fast** or **slow**. • When configuring the rate to **fast** mode, the period of sending LACP PDUs from the peer member interface is 1 second. If local member interface does not receive LACP PDU from the peer interface within 3 seconds (3 times the sending rate), the peer member interface will be considered unreachable and the status of the local member interface will be changed to Down immediately, and no more data will be forwarded through this interface. • When configuring the rate to **slow** mode, the period of sending LACP PDUs from the peer member interface is 30 seconds. The timeout of changing local interface status to Down is 90 seconds. The default rate mode is **slow**.

Example

- Enable LACP fast rate on interface xe-1/1/1.

```
admin@Xorplus# set protocols lacp interface xe-1/1/1 rate fast
admin@Xorplus# commit
```

run show lldp neighbor

The **run show lldp neighbor** command displays the neighbor device information of a specified interface or all the interfaces enabled LLDP.

Command Syntax

run show lldp neighbor [*<interface-name>* | **all**] [**detail**]

Parameter

Parameter	Description
[*<interface-name>* | **all**]	Optional. Specifies an interface name or **all**. **all** indicates to show the neighbor device information of all the interfaces enabled LLDP. If not specified, it will show the neighbor device information of all the interfaces enabled LLDP.
detail	Optional. Show details of the neighbor device information. If not specified, it will show the brief information of the neighbor device.

Example

- Display the details of neighbor device information of all the interfaces enabled LLDP.

```
admin@XorPlus# run show lldp neighbor all detail
Local Port: te-1/1/1
LLDP info:
--------------------------------------------------------------------------------
  Time To Live: 106
  Chassis Id: 68:21:5F:7F:10:C6
  Port ID: te-1/1/1
  Port Description: te-1/1/1
  System Name: PICOS
  System Description: Pica8, Inc.,AS5835_54T, PICOS 4.3.2/9b1219e332
  System Capability: B, RBridge, Router
  System Enabled Capability: Bridge, Router
  Management Address: 10.10.51.12
  Default VLAN ID: 1
  Auto Negotiation: Supported, Enabled
  Physical media capabilities: Others, 10base_T, 100base_TX, 100base_TXFD, 1000base_T, 1000base_TFD
  Media Attachment Unit type: 1000base_T_Full_Duplex
  802.3 Power via MDI :Not available

LLDP MED is not Enabled.

Total entries displayed: 1
```

set protocols dhcp6 snooping vlan

The **set protocols dhcp6 snooping vlan disable** command enables DHCPv6 snooping in a specified VLAN.

Command Syntax

set protocols dhcp6 snooping vlan <*vlan-id*> **disable** <**true** | **false**>

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
disable <**true**	**false**>	Enables or disables DHCPv6 snooping, the value could be **true** or **false**: • **true**: Disables DHCPv6 snooping. • **false**: Enables DHCPv6 snooping. By default, DHCPv6 snooping is disabled.

Usage Guidelines

DHCPv6 snooping should be enabled in the VLAN, it takes effect only on the DHCPv6 messages received from the VLAN enabled with DHCPv6 snooping function. Packets received from the VLANs with DHCPv6 snooping disabled will not be processed by the DHCPv6 snooping module, and they will be processed and forwarded by the device as ordinary packets.

NOTE:

- The DHCPv6 snooping function is only practicable to the clients directly connected to the local L2 domain, rather than connected through a router.
- When DHCPv6 snooping is disabled, the DHCPv6 binding entry for the VLAN will be removed correspondingly.

Example

- Enable DHCPv6 snooping in VLAN 12.

```
admin@Xorplus# set protocols dhcp6 snooping vlan 12 disable false
admin@Xorplus# commit
```

set protocols dhcp6 snooping trust-port

The **set protocols dhcp6 snooping trust-port** command configures an interface as a trust interface for DHCPv6 snooping.

Command Syntax

set protocols dhcp6 snooping trust-port <*interface-name*>

Parameters

Parameter	Description
trust-port <*interface-name*>	Specifies an interface name. The interface can be either a physical interface or an aggregated interface. By default, all interfaces are untrusted interfaces.

Usage Guidelines

In order to make the DHCPv6 client obtain an IP address from a legitimate DHCPv6 server, the device interface directly or indirectly connected to the DHCPv6 server trusted by the administrator must be set to the trust interface, so as to prevent a spoofing DHCPv6 server from assigning an IP address to the DHCPv6 client.

The trusted interface forwards DHCPv6 packets received from the DHCPv6 server normally, whereas the untrusted interface discards DHCPv6 packets received from the DHCPv6 server.

Example

- Configure ge-1/1/1 as trust port for DHCPv6 snooping.

```
admin@Xorplus# set protocols dhcp6 snooping trust-port ge-/1/1/1
admin@Xorplus# commit
```

set protocols dhcp6 snooping binding file

The **set protocols dhcp6 snooping binding file** command configures a DHCPv6 snooping binding file for synchronizing DHCPv6 snooping entries from memory.

Command Syntax

set protocols dhcp6 snooping binding file <*file-path*>

Parameters

Parameter	Description
file <*file-path*>	Specifies a file path to save the DHCPv6 snooping binding table.

Usage Guidelines

If a DHCPv6 snooping binding file is specified, the DHCPv6 snooping entries will be synchronized from the memory to the binding file. This prevents DHCPv6 snooping entries data loss in case of power failure. By setting a DHCPv6 snooping binding file, the system can directly load the existing snooping entries from the binding file after if recovers.

For non-X86 devices, the path of the binding file is **/mnt/open/dhcp6_bind**; for X86 devices, the binding file path should not be under **/tmp**.

Example

- Configure the DHCPv6 snooping binding file.

```
admin@Xorplus# set protocols dhcp6 snooping binding file /mnt/open/dhcp6_bind
admin@XorPlus# commit
```

set protocols dhcp6 snooping binding write-delay

The **set protocols dhcp6 snooping binding write-delay** command configures a delay timer for writing the DHCPv6 snooping entries from memory to the binding file.

Command Syntax

set protocols dhcp6 snooping binding write-delay <*write-delay-timer*>

Parameters

Parameter	Description
write-delay <*write-delay-timer*>	Specifies a delay timer for writing the DHCPv6 snooping entries from the memory to the binding file. The value is an integer in seconds that ranges from 15 to 86400. The default value is 300s.

Usage Guidelines

In order to reduce the system burden caused by frequent file writes, you can configure a delay timer for writing the DHCPv6 snooping entries from memory to the binding file.

NOTE:

In the case when the DHCPv6 snooping entry is changed by the administrator configuration modifications from the CLI, such as modifying the VLAN, the binding file will be immediately refreshed rather than wait for write-delay timer.

Example

- Configure a delay timer for writing the DHCPv6 snooping entries from memory to the binding file.

```
admin@Xorplus# set protocols dhcp6 snooping binding write-delay 24
admin@XorPlus# commit
```

set protocols dhcp6 snooping vlan option-policy

The **set protocols dhcp6 snooping vlan option-policy** command configures how to handle the Option field when receiving a DHCPv6 message on VLANs where DHCPv6 snooping is enabled.

Command Syntax

set protocols dhcp6 snooping vlan <*vlan-id*> **option-policy <drop | keep | insert | replace>**

Parameters

Parameter	Description
vlan <*vlan-id*>	Specifies a VLAN. The value is an integer that ranges from 1 to 4094.
option-policy <**drop	keep	insert	replace>**	Specifies the policy for Option. The value could be **drop**, **keep**, **insert** or **replace**. • **drop**: drop the packet if have Option 18 or Option 37 field. If the received DHCPv6 packets without Option 18 or Option 37 values, the packets will be forwarded. • **keep**: Option 18 and Option 37 in the packet remain unchanged and forwarded. • **insert**: the existing Option 18 or Option 37 remain unchanged; else, insert Option 18 or Option 37 with the value the administrator configured if not exist, then forwarding the packet to the DHCP server. • **replace**: The existing Option 18 and Option 37 will be replaced with the value administrator configured, then forwarded; Else, if not exist, the system inserts Option 18 or Option 37 with the value the administrator configured . The default value is **keep**.

Usage Guidelines

Option policy is used when receiving a DHCPv6 message from the DHCPv6 client. When option policy is set to “insert” or “replace”, you can use the following commands to set the format of interface ID and remote ID sub-options:

set protocols dhcp6 snooping option18 interface-id <port-index | port-name | port-description>
set protocols dhcp6 snooping option37 remote-id <*remote-id*>

Example

- Configure the Option policy.

```
admin@Xorplus# set protocols dhcp6 snooping vlan 12 option-policy insert
admin@Xorplus# commit
```

set protocols dhcp6 snooping option37 remote-id

The **set protocols dhcp6 snooping option37 remote-id** command configures the format of sub-option remote ID inserted into the Option 37 field for DHCPv6 snooping.

NOTE: The sub-option remote ID is applied to VLANs where option-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp6 snooping option37 remote-id <*remote-id*>

Parameters

Parameter	Description
remote-id <*remote-id*>	Specifies the type of remote ID in the Option 37 field. The value is a string. By default, the sub-option remote ID is not configured which means remote ID is not enabled.

Usage Guidelines

If configured, the remote-id field may be used to encode, for instance:

o a "caller ID" telephone number for dial-up connection
o a "user name" prompted for by a Remote Access Server
o a remote caller ATM address
o a "modem ID" of a cable data modem
o the remote IP address of a point-to-point link
o a remote X.25 address for X.25 connections
o an interface or port identifier

Example

- Configure the type of sub-option remote ID inserted into the DHCPv6 Option 37 field.

```
admin@Xorplus# set protocols dhcp6 snooping option37 remote-id Xorplus
```

set protocols dhcp6 snooping option18 interface-id

The **set protocols dhcp6 snooping option18 interface-id** command configures the format of sub-option interface ID inserted into the Option 18 field for DHCPv6 snooping.

NOTE: The sub-option interface ID is applied to VLANs where option-policy is set to “insert” or “replace”.

Command Syntax

set protocols dhcp6 snooping option18 interface-id <port-index | port-name | port-description>

Parameters

Parameter	Description
interface-id <port-index | port-name | port-description>	Specifies the type of interface ID in the Option 18 field. The value could be **port-index**, **port-name** or **port-description**. By default, the sub-option interface ID is not configured which means interface ID is not enabled.

Usage Guidelines

If configured, the interface ID is filled with the port identifier and VLAN.

- When “port-index” is selected, the format of the interface ID is “VLAN ID + port index”.
- When “port-name” is selected, the format of the interface ID is “VLAN ID + port name”.
- When “port-description” is selected, the format of the interface ID is “VLAN ID + port description”. The value of “port-description” can be set by the following commands:

set interface aggregate-ethernet <*lag_name*> **description** <*description*>

set interface gigabit-ethernet <*physical-port*> **description** <*description*>

Example

- Configure the format of the sub-option interface ID for the Option 18 field.

```
admin@Xorplus# set protocols dhcp6 snooping option18 interface-id port-index
admin@Xorplus# commit
```

set protocols dhcp6 snooping interface max-clients

The **set protocols dhcp6 snooping interface max-clients** command configures the maximum number of supported DHCPv6 clients accessed to physical port according to network status.

> When the number of clients in the DHCPv6 snooping binding table reaches this maximum value on this interface, any exceeding DHCPv6 packets will be discarded.

Command Syntax

set protocols dhcp6 snooping interface interface <*interface-name*> **max-clients** <*max-number*>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value could be a physical port.
max-clients <*max-number*>	Specifies maximum number of supported users. The value is an integer that ranges from 1 to 2048. The default value is 1024.

Example

- Configure the maximum number of supported DHCPv6 clients accessed to physical port according to network status.

```
admin@Xorplus# set protocols dhcp6 snooping interface ge-1/1/1 max-clients 2000
admin@Xorplus# commit
```

run show dhcp6 snooping binding

The **run show dhcp6 snooping binding** command displays the DHCPv6 snooping binding table, which includes the user MAC address, IP address, VLAN ID, access interface and the lease time.

Command Syntax

run show dhcp6 snooping binding

Parameter

None.

Example

- Show the DHCPv6 snooping binding table.

```
admin@Xorplus# run show dhcp6 snooping binding
Total count:     2
MAC Address     IPv6 Address     Port            VLAN ID   Lease(sec)
-------------------------------------------------------------------------------------------
e4:f0:04:89:b6:46  0        ae65           1         0/0
14:18:77:18:2c:b9   2::1       ae25           125       599/600
```

Table 1. Description of the run show dhcpv6 snooping binding command output

Item	Description
Mac Address	User MAC address.
IPv6 Address	User IPv6 address.
Port	User access interface.
VLAN ID	User VLAN ID.
Lease(sec)	Lease time for the IP address, in seconds. The format displayed is **Remaining Lease Time/Total Lease Time**.

set protocols dhcp6 guard policy device-role

The **set protocols dhcp6 guard policy device-role** command can set the device role to client or server.

The **delete protocols dhcp6 guard policy device-role** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **device-role <server | client>**

delete protocols dhcp6 guard policy <*policy-name*> **device-role**

Parameter

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
device-role <server | client>	Set the device role to client or server. The value could be **server** or **client**. **sever**: Set the device role to server. **client**: Set the device role to client. By default, the device role is **client**.

Example

- Set the device role of guard policy p1 to server.

```
admin@PICOS# set protocols dhcp6 guard policy p1 device-role server
admin@PICOS# commit
```

set protocols dhcp6 guard policy trust-port

The **set protocols dhcp6 guard policy trust-port** command can set the guard policy to trust port.

The **delete protocols dhcp6 guard policy trust-port** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **trust-port**

delete protocols dhcp6 guard policy <*policy-name*> **trust-port**

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.

Example

- Set the guard policy p1 to trust port.

```
admin@PICOS# set protocols dhcp6 guard policy p1 trust-port
admin@PICOS# commit
```

set protocols dhcp6 guard policy interface

The **set protocols dhcp6 guard policy interface** command can configure guard policy on an interface.

The **delete protocols dhcp6 guard policy interface** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **interface** <*interface-name*>

delete protocols dhcp6 guard policy <*policy-name*> **interface** <*interface-name*>

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
interface <*interface-name*>	Specifies the interface name. The value is a physical port or an LAG port.

Example

- Configure guard policy p1 on interface ge-1/1/2.

```
admin@PICOS# set protocols dhcp6 guard policy p1 interface ge-1/1/2
admin@PICOS# commit
```

set protocols dhcp6 guard policy preference-min

The **set protocols dhcp6 guard policy preference-min** command can set the minimum preference value for Advertise packets to allow forwarding.

The **delete protocols dhcp6 guard policy preference-min** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **preference-min** <*min-value*>

delete protocols dhcp6 guard policy <*policy-name*> **preference-min**

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
preference-min <*min-value*>	Specifies the minimum preference value. The value is an integer that ranges from 0 to 255. By default, the minimum preference value is 0.

Example

- Set the minimum preference value of guard policy p1 to 10.

```
admin@PICOS# set protocols dhcp6 guard policy p1 preference-min 10
admin@PICOS# commit
```

set protocols dhcp6 guard policy preference-max

The **set protocols dhcp6 guard policy preference-max** command can set the maximum preference value for Advertise packets to allow forwarding.

The **delete protocols dhcp6 guard policy preference-max** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **preference-max** <*max-value*>

delete protocols dhcp6 guard policy <*policy-name*> **preference-max**

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
preference-max <*max-value*>	Specifies the maximum preference value. The value is an integer that ranges from 0 to 255. By default, the maximum preference value is 255.

Example

- Set the maximum preference value of guard policy p1 to 200.

```
admin@PICOS# set protocols dhcp6 guard policy p1 preference-max 200
admin@PICOS# commit
```

set protocols dhcp6 guard policy match server source-address

The **set protocols dhcp6 guard policy match server source-address** command can set the server source-address for Advertise packets to allow forwarding.

The **delete protocols dhcp6 guard policy match server source-address** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **match server source-address** <*IPv6Net*>

delete protocols dhcp6 guard policy <*policy-name*> **match server source-address** <*IPv6Net*>

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
source-address <*IPv6Net*>	Specifies the server source-address. The value is an IPv6 address.

Example

- Set the server source-address of guard policy p1 to 2001::1/128.

```
admin@PICOS# set protocols dhcp6 guard policy p1 match server source-address 2001::1/128
admin@PICOS# commit
```

set protocols dhcp6 guard policy match reply ia-prefix

The **set protocols dhcp6 guard policy match reply ia-prefix** command can set the ia-prefix for Reply packets to allow forwarding.

The **delete protocols dhcp6 guard policy match reply ia-prefix** command deletes the configuration.

Command Syntax

set protocols dhcp6 guard policy <*policy-name*> **match reply ia-prefix** <*IPv6Net*>

delete protocols dhcp6 guard policy <*policy-name*> **match reply ia-prefix** <*IPv6Net*>

Parameters

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.
ia-prefix <*IPv6Net*>	Specifies the ia-prefix. The value is an IPv6 address.

Example

- Set the ia-prefix for Reply packets of guard policy p1 to 3001::0/64.

```
admin@PICOS# set protocols dhcp6 guard policy p1 match reply ia-prefix 3001::0/64
admin@PICOS# commit
```

run show dhcp6 guard policy

The **run show dhcp6 guard policy** command shows the information of the dhcp6 guard policy configuration.

Command Syntax

run show dhcp6 guard policy <*policy-name*>

Parameter

Parameter	Description
policy <*policy-name*>	Specifies the guard policy. The value is a policy name.

Example

- View the information of the dhcp6 guard policy configuration.

```
admin@PICOS# run show dhcp6 guard policy p1
dhcp6 guard policy: p1
    match:
        server source-address: 2001::/64
              reply ia-prefix: 3001::/64
    preference-max: 255
    preference-min: 0
    device role: server
    interface: ge-1/1/1
```

run show dhcp6 guard

The **run show dhcp6 guard** command shows the information of the dhcp6 guard configuration.

Command Syntax

run show dhcp6 guard

Parameter

None.

Example

- View the information of the dhcp6 guard configuration.

```
admin@PICOS# run show dhcp6 guard
dhcp6 guard policy: p1
    match:
        server source-address: 2001::/64
              reply ia-prefix: 3001::/64
    preference-max: 255
    preference-min: 0
    device role: server
    interface: ge-1/1/1
dhcp6 guard policy: p2
    device role: client
    interface: ge-1/1/2
```

IP Multicast Commands

- IGMP Snooping Configuration Commands
  - run show igmp-snooping
  - run show igmp-snooping groups
  - run show igmp-snooping mrouter
  - run show igmp-snooping querier
  - set protocols igmp-snooping enable
  - set protocols igmp-snooping interface max-groups
  - set protocols igmp-snooping last-member-query-count
  - set protocols igmp-snooping last-member-query-interval
  - set protocols igmp-snooping max-response-time
  - set protocols igmp-snooping query-interval
  - set protocols igmp-snooping report-suppression
  - set protocols igmp-snooping robustness-variable
  - set protocols igmp-snooping vlan-id enable
  - set protocols igmp-snooping vlan-id fast-leave
  - set protocols igmp-snooping vlan-id mrouter interface
  - set protocols igmp-snooping vlan-id querier address
  - set protocols igmp-snooping vlan-id querier enable
  - set protocols igmp-snooping vlan-id querier other-querier-timer
  - set protocols igmp-snooping vlan-id querier version
  - set protocols igmp-snooping vlan-id static group interface
  - set protocols igmp-snooping vlan-id unregistered flood-all
- IGMP Commands
  - set protocols igmp interface
  - set protocols igmp interface join-group
  - set protocols igmp interface query-interval
  - set protocols igmp interface query-max-response-time
  - set protocols igmp interface version
  - run show igmp groups
  - run show igmp interface
- PIM Configuration Commands
  - set protocols pim ecmp
  - set protocols pim interface active-active
  - set protocols pim interface drpriority
  - set protocols pim interface hello holdtime
  - set protocols pim interface hello interval
  - set protocols pim interface sm
  - set protocols pim interface use-source
  - set protocols pim join-prune-interval
  - set protocols pim keep-alive-timer
  - set protocols pim packets
  - set protocols pim register-suppress-time
  - set protocols pim rp
  - set protocols pim spt-switchover infinity-and-beyond
  - set protocols pim ssm prefix-list
  - run show pim interface
  - run show pim rp-info
  - run show pim neighbor
  - run show pim upstream
  - run show mroute
  - mtrace
  - run show pim group-type
- Multicast Source Discovery Protocol (MSDP) Commands
  - set protocols msdp mesh-group source
  - set protocols msdp mesh-group member
  - run show msdp mesh-group
  - run show msdp peer
  - run show msdp sa
- Multicast VLAN Registration (MVR) Commands
  - run show igmp-snooping mvr mvlan
  - run show igmp-snooping mvr receiver-vlan
  - set protocols igmp-snooping vlan-id mvr receiver vlan-list

- set protocols igmp-snooping vlan-id mvr source group

IGMP Snooping Configuration Commands

- run show igmp-snooping
- run show igmp-snooping groups
- run show igmp-snooping mrouter
- run show igmp-snooping querier
- set protocols igmp-snooping enable
- set protocols igmp-snooping interface max-groups
- set protocols igmp-snooping last-member-query-count
- set protocols igmp-snooping last-member-query-interval
- set protocols igmp-snooping max-response-time
- set protocols igmp-snooping query-interval
- set protocols igmp-snooping report-suppression
- set protocols igmp-snooping robustness-variable
- set protocols igmp-snooping vlan-id enable
- set protocols igmp-snooping vlan-id fast-leave
- set protocols igmp-snooping vlan-id mrouter interface
- set protocols igmp-snooping vlan-id querier address
- set protocols igmp-snooping vlan-id querier enable
- set protocols igmp-snooping vlan-id querier other-querier-timer
- set protocols igmp-snooping vlan-id querier version
- set protocols igmp-snooping vlan-id static group interface
- set protocols igmp-snooping vlan-id unregistered flood-all

run show igmp-snooping

The **run show igmp-snooping** command shows the configuration information of IGMP snooping.

Command Syntax

run show igmp-snooping [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the configuration information of IGMP snooping.

```
admin@XorPlus# run show igmp-snooping
Global IGMP Snooping configuration:
----------------------------------------
IGMP snooping             : Enabled
Report suppression           : Enabled
Robustness variable          : 2
Router aging time            : 260
Max response time            : 10
Query interval               : 60
Last member query count      : 2
Last member query interval   : 2
```

- Show the IGMP snooping configuration of a specific VLAN.

```
admin@XorPlus# run show igmp-snooping vlan 1
Vlan 1:
--------------------------------------------
IGMP snooping                       : Enabled
IGMPv2 fast leave                   : Enabled
IGMP querier state                  : Enabled
IGMP querier source ip address      : 0.0.0.0
IGMP other querier timer            : 1
IGMP querier version                : 2
```

run show igmp-snooping groups

The **run show igmp-snooping groups** command shows information about multicast group member ports which is used for Layer 2 forwarding, namely, the Layer 2 forwarding table.

Command Syntax

run show igmp-snooping groups [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the information about multicast group member ports.

```
admin@XorPlus# run show igmp-snooping groups
Vlan      Group                   Port List          Type
--------  ------------------   -----------------   ----------------------
1         238.255.0.1             ge-1/1/2          Static
                                  ge-1/1/1          Mrouter
```

run show igmp-snooping mrouter

The **run show igmp-snooping mrouter** command shows the information about IGMP snooping router port.

Command Syntax

run show igmp-snooping mrouter [**vlan** <*vlan-id*>]

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the information about IGMP snooping router port.

```
admin@XorPlus# run show igmp-snooping mrouter
Vlan           Ports          Type
--------    -------------     ---------
1              ge-1/1/1       Static
```

run show igmp-snooping querier

The **run show igmp-snooping querier** command shows the configuration information and status of the querier in a VLAN.

Command Syntax

run show igmp-snooping querier vlan <*vlan-id*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Optional. Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.

Example

- Show the configuration information and status of the querier.

```
admin@XorPlus# run show igmp-snooping querier vlan 1
Vlan 1:   IGMP switch querier status
-------------------------------------------------------
admin state                   : Disabled
admin version                 : 2
source IP address             : 0.0.0.0
other querier timer           : 1
operational state             : Non-Querier
```

set protocols igmp-snooping enable

The **set protocols igmp-snooping enable** command is used to enable or disable the global IGMP snooping function.

Command Syntax

set protocols igmp-snooping enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true** | **false**>	Enable or disable the global IGMP snooping function. The value is **true** or **false**. • **true**: enables the global IGMP snooping function. • **false**: disables the global IGMP snooping function. The default value is **false**.

Usage Guidelines

To enable IGMP snooping, both global and VLAN-based IGMP snooping need to be configured.

- If only the global IGMP snooping is enabled, IGMP snooping in the VLAN is disabled by default. To enable IGMP snooping in a VLAN, you also need to enable the VLAN-based IGMP snooping function via **set protocols igmp-snooping vlan-id enable** command.
- After both global and VLAN-based IGMP snooping are enabled, it will take effect only on interfaces that have already been added to this VLAN enabled IGMP snooping.

Example

- Enable the global IGMP snooping function.

```
admin@Xorplus# set protocols igmp-snooping enable true
admin@Xorplus# commit
```

set protocols igmp-snooping interface max-groups

The **set protocols igmp-snooping interface max-groups** command configures the maximum number of static/dynamic multicast groups that a specific interface can join.

The **delete protocols igmp-snooping interface max-groups** command sets the maximum number of static/dynamic multicast groups on a specific interface to the default value of 256.

Command Syntax

set protocols igmp-snooping interface <*interface-name*> **max-groups** <*int*>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the physical interface name. The value is a string.
max-groups <*int*>	Specifies the maximum number of static/dynamic multicast groups on a specific interface. The value is an integer. Range: 1 to 256. Default: 256.

Usage Guidelines

By configuring this command, users can control the maximum number of static/dynamic multicast groups on a specific interface. If the number of Layer 2 multicast entries on the interface already exceeds the configured limit, the number of Layer 2 multicast entries on the interface does not change and the interface cannot learn new Layer 2 multicast entries.

The Layer 2 multicast table can be viewed by using the command **run show igmp-snooping groups**.

If the multicast groups number of an interface has already reached the configured max number of multicast groups, the system will report an error under the following two conditions:

- The system prints a warning message in the syslog when receiving IGMP packets with new multicast groups, prompting that the number of multicast groups on the interface exceeding the configured max number of multicast groups. For example,

```
Nov 11 2022 09:48:13 PICOS  local0.warning : [IGMPSNOOPING]The number of groups (6) reaches to the configured maxim
Nov 11 2022 09:48:14 PICOS  local0.warning : [IGMPSNOOPING]The number of groups (8) reaches to the configured maxim
```

- Users cannot configure anymore new static multicast groups when the number of multicast groups on an interface has already reached the configured max number of multicast groups. Commit fails with an error message "Already reach max multicast mac entries count : *value of max-groups*". For example,

```
admin@PICOS# set protocols igmp-snooping vlan-id 100 static group 224.1.2.2 interface te-1/1/23
admin@PICOS# commit
Already reach max multicast mac entries count : 256
Commit failed.
```

Example

- Configure the maximum number of static/dynamic multicast groups on interface te-1/1/24.

```
admin@PICOS# set protocols igmp-snooping interface te-1/1/24 max-groups 8
admin@PICOS# commit
```

set protocols igmp-snooping last-member-query-count

The **set protocols igmp-snooping last-member-query-count** command configures the number of times that the querier sends a group-specific query message.

Command Syntax

set protocols igmp-snooping last-member-query-count <*last-member-query-count*>

Parameter

Parameter	Description
last-member-query-count <*last-member-query-count*>	Specifies the number of times that the querier sends a group-specific query message. The value is an integer ranges from 1 to 7. The default value is 2.

Usage Guidelines

When the switch receives an IGMP leave message from a host, it sends the group-specific query messages to query whether the particular multicast group still has members and starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = last-member-query-count × last-member-query-interval **+** max-response-time. The **set protocols igmp-snooping last-member-query-count** command is used to configure the last-member-query-count in the above formula. The last-member-query-interval can be configured using the **set protocols igmp-snooping last-member-query-interval** command. The max-response-time can be configured using the **set protocols igmp-snooping max-response-time** command.

If the switch receives a report message from other hosts within the aging time, it continues to maintain memberships of the particular multicast group. However, if the switch receives no report message within the aging time, it will stop maintaining memberships of the particular multicast group and delete the particular multicast group entry in the Layer 2 forwarding table.

Example

- Configure the number of times that the querier sends a group-specific query message.

```
admin@Xorplus# set protocols igmp-snooping last-member-query-count 2
admin@Xorplus# commit
```

set protocols igmp-snooping last-member-query-interval

The **set protocols igmp-snooping last-member-query-interval** command configures the interval that the querier sends a group-specific query message.

Command Syntax

set protocols igmp-snooping last-member-query-interval <*last-member-query-interval*>

Parameter

Parameter	Description
last-member-query-interval <*last-member-query-interval*>	Specifies the interval of sending a particular multicast group query packet. The value is an integer, in seconds, that ranges from 1 to 32. The default value is 2.

Usage Guidelines

When the switch receives an IGMP leave message from a host, it sends the group-specific query messages to query whether the particular multicast group still has members and starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = last-member-query-count × last-member-query-interval **+** max-response-time. The **set protocols igmp-snooping last-member-query-count** command is used to configure the last-member-query-count in the above formula. The last-member-query-interval can be configured using the **set protocols igmp-snooping last-member-query-interval** command. The max-response-time can be configured using the **set protocols igmp-snooping max-response-time** command.

If the switch receives a report message from other hosts within the aging time, it continues to maintain memberships of the particular multicast group. If the switch receives no report message within the aging time, it will stop maintaining memberships of the particular multicast group and delete the particular multicast group entry in the Layer 2 forwarding table.

Example

- Configure the interval that the querier sends a group-specific query message.

```
admin@Xorplus# set protocols igmp-snooping last-member-query-interval 2
admin@XorPlus# commit
```

set protocols igmp-snooping max-response-time

The **set protocols igmp-snooping max-response-time** command configures the maximum response time for an IGMP general query message or a group-specific query message.

Command Syntax

set protocols igmp-snooping max-response-time <*max-response-time*>

Parameter

Parameter	Description
max-response-time <*max-response-time*>	Specifies the maximum response time for an IGMP general query message or a group-specific query message. The value is an integer, in seconds, that ranges from 1 to 25. The default value is 10.

Usage Guidelines

The maximum response time can be used to adjust the aging time of member ports. When the switch receives the report message from the downstream host, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count × General query interval + Maximum response time. The **set protocols igmp-snooping max-response-time** command is used to configure the maximum response time in the above formula. The General query count can be configured using the **set protocols igmp-snooping robustness-variable** command. The General query interval can be configured using the **set protocols igmp-snooping query-interval** command.

When the aging time of the member port expires, this member port will be deleted from the Layer 2 forwarding table.

When the switch receives an IGMP report message on the dynamic member port, the aging time of the member port will be reset.

The maximum response time can be used to adjust the aging time of member ports when the switch receives an IGMP leave message from a host, for detail please refer to **set protocols igmp-snooping last-member-query-count** command.

NOTE:

- We recommend setting the value of **Maximum response time** smaller than the value of **General query interval**.
- The aging time takes effect only on dynamic member ports, however, the static member ports do not age.

Example

- Configure the maximum response time for IGMP general query message.

```
admin@Xorplus# set protocols igmp-snooping max-response-time 10
admin@XorPlus# commit
```

set protocols igmp-snooping query-interval

The **set protocols igmp-snooping query-interval** command configures the interval of sending IGMP general query message.

Command Syntax

set protocols igmp-snooping query-interval <*query-interval*>

Parameter

Parameter	Description
max-response-time <*max-response-time*>	Specifies the interval of sending an IGMP general query message. The value is an integer, in seconds, that ranges from 1 to 18000. The default value is 60.

Usage Guidelines

The query interval can be used to adjust aging time of member ports. When the switch receives the report message from the downstream host, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count × General query interval + Maximum response time. The **set protocols igmp-snooping query-interval** command is used to configure the General query interval in the above formula. The General query count can be configured using the **set protocols igmp-snooping robustness-variable** command. The Maximum response time can be configured using the **set protocols igmp-snooping max-response-time** command.

When the aging time of the member port expires, this member port will be deleted from the Layer 2 forwarding table.

When the switch receives an IGMP report message on the dynamic member port, the aging time of the member port will be reset.

NOTE:

- We recommend setting the value of **Maximum response time** smaller than the value of **General query interval**.
- The aging time takes effect only on dynamic member ports, however, the static member ports do not age.

Example

- Configure the interval of sending IGMP general queries.

```
admin@Xorplus# set protocols igmp-snooping query-interval 60
admin@XorPlus# commit
```

set protocols igmp-snooping report-suppression

The **set protocols igmp-snooping report-suppression** command is used to enable or disable the IGMP snooping membership report suppression function.

Command Syntax

set protocols igmp-snooping report-suppression <**true | false**>

Parameter

Parameter	Description
report-suppression <**true	false**>	Enable or disable the membership report suppression function. The value is **true** or **false**. • **true**: enables the membership report suppression function. • **false**: disables the membership report suppression function. The default value is **false**.

Usage Guidelines

When IGMP snooping membership report suppression function is enabled, the Layer 2 device will forward only one IGMP report of a multicast group to the upstream device in suppression time of 1/2 of query time. The Layer 2 device will reset the suppression timer when receiving the first IGMP report message. Only when the first member joins a multicast group when a host sends a report message, the Layer 2 switch will forward the report message to the upstream device for creating or maintaining the multicast entry. This function helps to reduce the amount of IGMP snooping traffic in the network.

Example

- Enable the IGMP snooping membership report suppression function.

```
admin@Xorplus# set protocols igmp-snooping report-suppression true
admin@XorPlus# commit
```

set protocols igmp-snooping robustness-variable

The **set protocols igmp-snooping robustness-variable** command configures the IGMP robustness coefficient.

Command Syntax

set protocols igmp-snooping robustness-variable <*robustness-variable*>

Parameter

Parameter	Description
robustness-variable <*robustness-variable*>	Specifies the IGMP robustness coefficient. The value is an integer that ranges from 2 to 4. The default value is 2.

Usage Guidelines

The robustness coefficient can be used to adjust aging time of member ports. When the switch receives the report message from the downstream host, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count × General query interval + Maximum response time. The **set protocols igmp-snooping robustness-variable** command is used to configure the General query count in the above formula. The General query interval can be configured using the **set protocols igmp-snooping query-interval** command. The Maximum response time can be configured using the **set protocols igmp-snooping max-response-time** command.

When the aging time of the member port expires, this member port will be deleted from the Layer 2 forwarding table.

When the switch receives an IGMP report message on the dynamic member port, the aging time of the member port will be reset.

> **NOTE:**
> The aging time takes effect only on dynamic member ports whereas static member ports do not age.

Example

- Configure the IGMP robustness coefficient.

```
admin@Xorplus# set protocols igmp-snooping robustness-variable 2
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id enable

The Internet Group Management Protocol (IGMP) is used to establish multicast group membership on IPv4 networks, making it an important component of IP multicast. It is used for one-to-many applications such as video streaming and gaming. IGMP snooping involves the process of listening for IGMP traffic between hosts and routers, enabling a switch to learn which devices are involved in which IP multicast conversations. This enables multicasts to be filtered from links and ports where they're not needed, thus reducing network traffic. IGMP snooping is typically disabled by default on network switches. This document details how to enable IGMP if desired, on a per-VLAN basis.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **enable** <**true** | **false**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
enable <**true** | **false**>	Enable or disable the VLAN-based IGMP snooping function. The value is **true** or **false**. • **true**: enables the VLAN-based IGMP snooping function. • **false**: disables the VLAN-based IGMP snooping function. The default value is **false**.

Usage Guidelines

To enable IGMP snooping, both global and VLAN-based IGMP snooping need to be configured.

- If only the global IGMP snooping is enabled, IGMP snooping in the VLAN is disabled by default. To enable IGMP snooping in a VLAN, you also need to enable the VLAN-based IGMP snooping function via **set protocols igmp-snooping vlan-id enable** command.
- After both global and VLAN-based IGMP snooping are enabled, it will take effect only on interfaces that have already been added to this VLAN enabled IGMP snooping.

Example

- Enable the VLAN-based IGMP snooping function.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 enable true
admin@Xorplus# commit
```

set protocols igmp-snooping vlan-id fast-leave

The **set protocols igmp-snooping vlan-id fast-leave** command is used to enable or disable the fast leave function to allow member ports in a VLAN to quickly leave the multicast group.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **fast-leave** <**true | false**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
fast-leave <**true	false**>	Enable or disable the fast leave function. The value is **true** or **false**. • **true**: enables the fast leave function. • **false**: disables the fast leave function. The default value is **false**.

Usage Guidelines

Fast leave of a member port means that the switch will delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives an IGMP leave message for the group, instead of waiting for the member port to age.

NOTE:

When there are multiple receiver hosts under an interface, this function may interrupt other hosts in the same multicast group in receiving multicast data. So, it is recommended to disable the fast leave function in this scenario.

Example

- Enable the fast leave function to allow member ports in a VLAN to quickly leave the multicast groups.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 fast-leave true
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id mrouter interface

The **set protocols igmp-snooping vlan-id mrouter interface** command configures the interface as a static router port in the specified VLAN.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **mrouter interface** <*interface-name*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
interface <*interface-name*>	Specifies the interface of the switch as a static router port.

Usage Guidelines

If you need to forward IGMP report / leave packets from one interface to the upstream IGMP querier permanently and stably, you can configure the interface as a static router port. Static router port will not be affected by the aging time, it will not age.

Example

- Configure the interface as a static router port in the specified VLAN.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 mrouter interface ge-1/1/3
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier address

The **set protocols igmp-snooping vlan-id querier address** command configures the source IP address of the general query message and group-specific query message sent by the querier.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier address** <*querier-address*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
querier address <*querier-address*>	Specifies a source IP address. The value is in dotted decimal notation. The default value is 0.0.0.0.

Usage Guidelines

After the Layer 2 device enables the querier function, you can run this command to configure the source IP address of the general query message and group-specific query message sent by the querier.

Example

- Configure the source IP address of the general query message and group-specific query message sent by the querier.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier address 192.168.10.2
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier enable

The **set protocols igmp-snooping vlan-id querier enable** command is used to enable or disable the querier function in a VLAN.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier enable** <**true | false**>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
enable <**true	false**>	Enable or disable the querier function in a VLAN. The value is **true** or **false**. • **true**: enables the querier function in a VLAN. • **false**: disables the querier function in a VLAN. The default value is **false**.

Usage Guidelines

When a Layer 3 multicast device is not running the IGMP protocol or in a pure Layer 2 network, IGMP snooping querier can be configured on a Layer 2 device to send IGMP query messages.

Example

- Enable the querier function in a VLAN.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier enable true
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier other-querier-timer

The **set protocols igmp-snooping vlan-id querier other-querier-timer** command configures the IGMP snooping querier other-querier-timer.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier other-querier-timer** <*other-querier-timer*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
other-querier-timer <*other-querier-timer*>	Specifies the IGMP snooping querier other-querier-timer. The value is an integer, in seconds, that ranges from 1 to 1000. The default value is 120.

Usage Guidelines

You can enable IGMP snooping querier function on the Layer 2 device to send IGMP query messages to take the querier role similar to Layer 3 multicast devices. If the Layer 2 querier receives an IGMP general query message sent by the upstream Layer 3 querier device, it will forward the IGMP general query message to all ports excluding the port receiving the messages of the VLAN. The IGMP snooping general query packets originally produced and planned to be sent by the Layer 2 querier devices are delayed and will be sent after the time of other-querier-timer.

Example

- Configure the IGMP snooping querier other-querier-timer.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier other-querier-timer 12
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id querier version

The **set protocols igmp-snooping vlan-id querier version** command configures the IGMP message version that the querier can support.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **querier version** <*querier-version*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
querier version <*querier-version*>	Specifies the IGMP message version that the querier supports. The value is **1** or **2**. • **1**: indicates that the querier processes only IGMPv1 messages. • **2**: indicates that the querier processes IGMPv1 and IGMPv2 messages. The default value is **2**.

Example

- Configure the IGMP snooping querier version.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 querier version 1
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id static group interface

The **set protocols igmp-snooping vlan-id static group interface** command configures a static member port to the particular multicast group.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **static group** <*group-address*> **interface** <*interface-name*>

Parameter

Parameter	Description
vlan-id <*vlan-id*>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
group <*group-address*>	Specifies the IP address of a multicast group. The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
interface <*interface-name*>	Specifies the interface of the switch as a static member interface.

Usage Guidelines

In addition to dynamically establishing a multicast forwarding table through Layer 2 multicast protocols, you can manually configure the Layer 2 multicast forwarding entries to statically bind interfaces to multicast groups. After an interface is statically added to a multicast group, users on the interface can receive multicast data in the multicast group permanently and stably. Static member port will not be affected by the aging time, it will not age.

Example

- Configure a static member interface to the multicast group.

```
admin@XorPlus# set protocols igmp-snooping vlan-id 2 static group 224.0.0.1 interface ge-1/1/3
admin@XorPlus# commit
```

set protocols igmp-snooping vlan-id unregistered flood-all

The **set protocols igmp-snooping vlan-id unregistered flood-all** command can be used to enable or disable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **unregistered flood-all** <**true | false**>

Parameters

Parameter	Description
vlan-id <*vlan-id*>	Specifies the VLAN tag identifier. The valid VLAN ID range is 1-4094.
enable <**true	false**>	Enable or disable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled. • **true**: Enable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled. • **false**: Disable unknown multicast traffic flooding in a VLAN with IGMP snooping enabled. This function is disabled by default. Unknown multicast traffic can be forwarded to the router ports.

Example

- Enable unknown multicast traffic flooding in VLAN 100 with IGMP snooping enabled.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 100 unregistered flood-all true
admin@Xorplus# commit
```

IGMP Commands

- set protocols igmp interface
- set protocols igmp interface join-group
- set protocols igmp interface query-interval
- set protocols igmp interface query-max-response-time
- set protocols igmp interface version
- run show igmp groups
- run show igmp interface

set protocols igmp interface

The **set protocols igmp interface** command enables IGMP on an L3 interface.

Command Syntax
set protocols igmp interface <*interface-name*>
delete protocols igmp interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.

Usage Guidelines

On a shared network segment, user hosts and Layer 3 multicast devices directly connected to the user network segment must run IGMP. A multicast device can process IGMP messages sent from user hosts only after IGMP is enabled on the interfaces connected to user network segments.

Example
• This example enables IGMP on vlan2:

```
admin@XorPlus# set protocols igmp interface vlan2
admin@XorPlus# commit
```

set protocols igmp interface join-group

The **set protocols igmp interface join-group** command configures a static multicast group on an L3 interface.

Command Syntax
set protocols igmp interface <*interface-name*> **join-group** <*group-address*> [**source** <*source-address*>]

delete protocols igmp interface <*interface-name*> **join-group** <*group-address*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
join-group <*group-address*>	Specifies a multicast group address. In batch configuration mode, this parameter specifies the start address of the multicast group range. The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
source <*source-address*>	Optional. Specifies a multicast source address. If the specified static group address is an SSM group address, you must specify a multicast source address for the group. The address is in dotted decimal notation.

Usage Guidelines

You can configure static multicast groups on user-side interfaces of the switch in some scenarios, for example:

- There are long-term group members on a shared network segment, and the switch needs to forward multicast data to these group members quickly and steadily.
- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the switch considers that the multicast group always has members on the network segment of the interface. Therefore, the switch always forwards multicast data of the multicast group.

Note that: The IGMP entries of static groups configured on an interface never time out. The switch considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment of the interface.

Example
• Configure static multicast group 224.1.1.1 on vlan2.

```
admin@XorPlus# set protocols igmp interface vlan2 join-group 224.1.1.1
admin@XorPlus# commit
```

set protocols igmp interface query-interval

The **set protocols igmp interface query-interval** command sets the interval at which an L3 interface sends IGMP General Query messages.

Command Syntax
set protocols igmp interface <*interface-name*> **query-interval** <*query-interval*>

delete protocols igmp interface <*interface-name*> **query-interval**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
query-interval <*query-interval*>	Specifies the interval at which an interface sends IGMP General Query messages. The value is an integer that ranges from 1 to 1800, in seconds.

Usage Guidelines

An IGMP querier sends IGMP General Query messages at an interval to check whether a local network segment has group members. This interval is the general query interval. You can set the general query interval based on situations on your network.

Example
• Configure the interval at which an interface sends IGMP General Query messages to 50 seconds on vlan2.

```
admin@XorPlus# set protocols igmp interface vlan2 query-interval 50
admin@XorPlus# commit
```

set protocols igmp interface query-max-response-time

The **set protocols igmp interface query-max-response-time** command sets the maximum response time for IGMP General Query messages on an interface.

Command Syntax
set protocols igmp interface <*interface-name*> **query-max-response-time** <*interval*>

delete protocols igmp interface <*interface-name*> **query-max-response-time**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
query-max-response-time <*interval*>	Specifies the maximum response time for IGMP General Query messages. The value is an integer that ranges from 10 to 250, in deciseconds.

Usage Guidelines

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large number of Report messages sent from many hosts at the same time. The network may be congested when this situation occurs.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

Example
• Set the maximum response time for IGMP General Query messages to 80 deciseconds on vlan2.

```
admin@XorPlus# set protocols igmp interface vlan2 query-max-response-time 80
admin@XorPlus# commit
```

set protocols igmp interface version

Users can configure IGMP protocol version for a specified L3 interface.

Command Syntax
set protocols igmp interface <*interface-name*> **version** <*number*>
delete protocols igmp interface <*interface-name*> **version**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.
version <*number*>	The IGMP protocol version. The value could be **2** or **3**.

Usage Guidelines

The switch can identify IGMP messages of a version earlier than its own IGMP version but cannot identify IGMP messages of a later version. To ensure normal IGMP operation, ensure that the switch runs the same IGMP version as member hosts or a later IGMP version.

If multiple switches exist on a shared network segment, configure the same IGMP version on all switch interfaces connected to hosts. Otherwise, errors may occur in IGMP operation because interfaces running different IGMP versions send packets with different formats.

Example
• This example sets IGMP protocol version to 2 on vlan2:

```
admin@XorPlus# set protocols igmp interface vlan2 version 2
admin@XorPlus# commit
```

run show igmp groups

The **run show igmp groups** command displays information about all IGMP groups that hosts have joined by sending IGMP Report messages.

Command Syntax
run show igmp groups

Parameter

None.

Example
• Display information about all IGMP groups.

```
admin@XorPlus# run show igmp groups
Total IGMP groups: 6
Watermark warn limit(Not Set): 0
Interface        Address         Group           Mode Timer    Srcs V Uptime
vlan2            10.10.60.10      224.0.0.2       INCL --:--:--    1 2 01:12:11
vlan2            10.10.60.10      224.0.0.22      INCL --:--:--    1 2 01:12:11
vlan2            10.10.60.10      238.255.0.1     INCL --:--:--    1 2 01:12:11
vlan3            10.10.61.10      224.0.0.2       INCL --:--:--    1 3 01:33:28
vlan3            10.10.61.10      224.0.0.22      INCL --:--:--    1 3 01:33:28
vlan3            10.10.61.10      238.255.0.2     INCL --:--:--    1 3 01:33:28
```

run show igmp interface

The **run show igmp interface** command displays information about IGMP interfaces.

Command Syntax
run show igmp interface [<*interface-name*>]

Parameter

Parameter	Description
<*interface-name*>	Optional. Specifies the VLAN interface name, the loopback interface name, the routed interface or the sub-interface name. The value is a string.

Example

- Display the IGMP configuration and running information on VLAN771.

```
admin@XorPlus# run show igmp interface vlan771
Interface : vlan771
State     : up
Address   : 71.1.1.166
Uptime    : 00:11:18
Version   : 3


Querier
-------
Querier     : local
Start Count : 0
Query Timer : 00:01:43
Other Timer : --:--:--


Timers
------
Group Membership Interval      : 260s
Last Member Query Count        : 2
Last Member Query Time         : 2s
Older Host Present Interval    : 260s
Other Querier Present Interval : 255s
Query Interval                 : 125s
Query Response Interval        : 10s
Robustness Variable            : 2
Startup Query Interval         : 31s


Flags
-----
All Multicast   : no
Broadcast       : yes
Deleted         : no
Interface Index : 52
Multicast       : yes
Multicast Loop  : 0
Promiscuous     : no
```

- Display information about all IGMP interfaces.

```
admin@XorPlus# run show igmp interface
```

```
Interface         State          Address  V  Querier  Query Timer    Uptime
vlan2              up        10.10.60.10  2    local     00:00:40  02:13:12
vlan3              up        10.10.61.10  3    local     --:--:--  00:36:29
```

PIM Configuration Commands

- set protocols pim ecmp
- set protocols pim interface active-active
- set protocols pim interface drpriority
- set protocols pim interface hello holdtime
- set protocols pim interface hello interval
- set protocols pim interface sm
- set protocols pim interface use-source
- set protocols pim join-prune-interval
- set protocols pim keep-alive-timer
- set protocols pim packets
- set protocols pim register-suppress-time
- set protocols pim rp
- set protocols pim spt-switchover infinity-and-beyond
- set protocols pim ssm prefix-list
- run show pim interface
- run show pim rp-info
- run show pim neighbor
- run show pim upstream
- run show mroute
- mtrace
- run show pim group-type

set protocols pim ecmp

The **set protocols pim ecmp** command is used to enable ECMP function for PIM.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] ecmp [rebalance]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Usage Guidelines

- If pim has the a choice of ECMP nexthops for a particular RPF, pim will cause S,G flows to be spread out amongst the nexthops. If this command is not specified then the first nexthop found will be used. This command is vrf aware, to configure for a vrf, specify the vrf name.
- If pim is using ECMP and an interface goes down, cause pim to rebalance all S,G flows across the remaining nexthops. If this command is not configured pim only modifies those S,G flows that were using the interface that went down.

Example

- Enable ECMP function for PIM.

```
admin@Xorplus# set protocols pim ecmp
admin@Xorplus# commit
```

set protocols pim interface active-active

The **set protocols pim interface active-active** command is used to turn on PIM active-active configuration. This command will not do anything if you do not have the underlying ability of a MLAG implementation.

The **delete protocols pim interface active-active** command is used to disable PIM active-active configuration.

Command Syntax

set protocols pim interface <*interface-name*> **active-active**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.

Usage Guidelines

For a multicast sender or receiver to be supported over a dual-attached MLAG bond, you must configure pim active-active.

Example

- Set the PIM active-active configuration.

```
admin@Xorplus# set protocols pim interface vlan-2 active-active
admin@Xorplus# commit
```

set protocols pim interface drpriority

The **set protocols pim interface drpriority** command is used to configure the Designated Router priority per interface.

Command Syntax

set protocols pim interface <*interface-name*> **drpriority** <*dr-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
drpriority <*dr-priority*>	Specifies the Designated Router priority. The greater the value, the higher the priority. The value is an integer that ranges from 1 to 4294967295. The default value is 1.

Usage Guidelines

The DR election is based on the priority and the IP address. To elect the DR, the PIM neighbors send the Hello message that contains the DR priority to each other. The switch with the highest priority functions as the DR. If the switches have the same priority, the switch with the largest IP address functions as the DR.

Example

- Configure the Designated Router priority for the PIM interface vlan-2 to 100.

```
admin@Xorplus# set protocols pim interface vlan-2 drpriority 100
admin@Xorplus# commit
```

set protocols pim interface hello holdtime

The **set protocols pim interface hello holdtime** command is used to configure the randomized triggered delay of PIM Hello messages (in seconds) per interface.

Command Syntax

set protocols pims interface <*interface-name*> **hello holdtime** < *interval*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
hello holdtime < *interval*>	Specifies the maximum delay for triggering Hello messages. The value is an integer that ranges from 3 to 180 in seconds.

Usage Guidelines

To avoid the conflict caused by multiple PIM devices sending Hello message at the same time, the PIM device automatically selects a random number smaller than the configured value as the delay. When detecting Hello messages in the network, the PIM device sends Hello message after the delay.

When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and hello-triggered-delay. This prevents synchronization of Hello messages if multiple routers are powered on simultaneously. After the initial randomized interval, Hello messages must be sent every hello-period seconds.

Example

- Set the randomized triggered delay of PIM Hello messages to 10 seconds on vlan-2.

```
admin@Xorplus# set protocols pim interface vlan-2 hello holdtime 10
admin@Xorplus# commit
```

set protocols pim interface hello interval

The **set protocols pim interface hello interval** command configures the PIM Hello messages period (in seconds) per interface.

Command Syntax

set protocols pim interface <*interface-name*> **hello interval** <*interval*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
hello interval <*interval*>	Specifies the interval for sending Hello messages. The value is an integer that ranges from 1 to 180, in seconds.

Usage Guidelines

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the this command to set the interval for sending Hello messages. The neighbor holdtime is 3.5 * hello-period.

Example

- Set the interval for sending Hello messages to 40 seconds on vlan-2.

```
admin@Xorplus# set protocols pim interface vlan-2 hello interval 40
admin@Xorplus# commit
```

set protocols pim interface sm

The **set protocols pim interface sm** command is used to enable PIM-SM function on a specific L3 interface.

The **delete protocols pim interface sm** command is used to disable PIM-SM function on a specific L3 interface.

Command Syntax

set protocols pim interface <*interface-name*> **sm**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.

Example

- Enable PIM-SM function on the L3 VLAN interface vlan-2.

```
admin@Xorplus# set protocols pim interface vlan-2 sm
admin@Xorplus# commit
```

set protocols pim interface use-source

The **set protocols pim interface use-source** command is used to configure the source IP address.

Command Syntax

set protocols pim interface <*interface-name*> **use-source** <*source-ip*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an L3 interface. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.The value is a string.
use-source <*source-ip*>	Specifies the source IP address.

Usage Guidelines

If you have multiple addresses configured on a particular interface and would like pim to use a specific source address associated with that interface.

Example

- Configure the source IP address for the PIM interface vlan-2 to 192.168.10.1.

```
admin@Xorplus# set protocols pim interface vlan-2 use-source 192.168.10.1
admin@Xorplus# commit
```

set protocols pim join-prune-interval

The **set protocols pim join-prune-interval** command configures the frequency at which the router will send periodic join or prune-interval messages.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] join-prune-interval** <*INTERVAL-VALUE*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
join-prune-interval <*INTERVAL-VALUE*>	Specifies the join-prune-interval in seconds. Range 60 to 600.

Usage Guidelines

If pim has the a choice of ECMP nexthops for a particular RPF, pim will cause S,G flows to be spread out amongst the nexthops. If this command is not specified then the first nexthop found will be used. This command is vrf aware, to configure for a vrf, specify the vrf name.

Example

- Configure join prune interval:

```
admin@Xorplus# set protocols pim join-prune-interval 120
admin@Xorplus# commit
```

set protocols pim keep-alive-timer

The **set protocols pim keep-alive-timer** command modifies the time out value for a S,G flow from 31-60000 seconds.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] keep-alive-timer** <*INTERVAL*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
keep-alive-timer <*INTERVAL*>	Specifies the time out value for a S,G flow in seconds. Range 31 to 60000.

Usage Guidelines

31 seconds is chosen for a lower bound because some hardware platforms cannot see data flowing in better than 30 second chunks. This command is vrf aware, to configure for a vrf, specify the vrf name.

Example

- Configure the time out value for a S,G flow.

```
admin@Xorplus# set protocols pim keep-alive-timer 120
admin@Xorplus# commit
```

set protocols pim packets

The **set protocols pim packets** command configures the max number of packets incoming that can be processed at one time when processing packets from a neighbor.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] packets** <*packets-number*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
keep-alive-timer <*INTERVAL*>	Specifies the max number of packets incoming that can be processed at one time. The value is an integer that ranges from 1 to 100.

Usage Guidelines

When processing packets from a neighbor process the number of packets incoming at one time before moving on to the next task. The default value is 3 packets. This command is only useful at scale when you can possibly have a large number of pim control packets flowing. This command is vrf aware, to configure for a vrf, specify the vrf name.

Example

- Configure the max number of packets incoming that can be processed at one time.

```
admin@Xorplus# set protocols pim packets 50
admin@Xorplus# commit
```

set protocols pim register-suppress-time

The **set protocols pim register-suppress-time** command modifies the time that PIM will register suppress a FHR will send register notifications to the kernel.

Command Syntax

set protocols pim [vrf<*vrf-name*>**] register-suppress-time** <*interval*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
register-suppress-time <*interval*>	Specifies the register suppress time. The value is an integer in seconds that ranges from 5 to 60000.

Example

- Configure the register suppress time.

```
admin@Xorplus# set protocols pim register-suppress-time 50
admin@Xorplus# commit
```

set protocols pim rp

The **set protocols pim rp** command statically configures a static RP for a specified multicast group.

Command Syntax

set protocols pim [vrf<*vrf-name*>] rp <*rp-address*> [**group** <*group-address*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
rp <*rp-address*>	Specifies the address of the static RP in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
group <*group-address*>	Optional. Specifies the multicast group address in IPv4/prefix-lenghth format.

Usage Guidelines

This command must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all IPv4 multicast addresses (224.0.0.0 - 239.255.255.255).

Example

- Configure the router as the RP.

```
admin@Xorplus# set protocols pim rp 10.110.0.6
admin@Xorplus# commit
```

set protocols pim spt-switchover infinity-and-beyond

The **set protocols pim spt-switchover** command configures SPT switchover on a per-group basis, allowing for some groups to never switch to a shortest path tree.

Command Syntax

set protocols pim [vrf<*vrf-name*>] spt-switchover infinity-and-beyond prefix-list <*prefix-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
prefix-list <*prefix-list*>	Specifies the prefix-list name. The value is a string which has been set by comannd set routing prefix-list.

Usage Guidelines

When the LHR receives the first multicast packet, it sends a PIM (S,G) join towards the FHR to efficiently forward traffic through the network. This builds the shortest path tree (SPT), or the tree that is the shortest path to the source. When the traffic arrives over the SPT, a PIM (S,G) RPT prune is sent up the shared tree towards the RP. This removes multicast traffic from the shared tree; multicast data is only sent over the SPT.

You can configure SPT switchover on a per-group basis, allowing for some groups to never switch to a shortest path tree; this is also called SPT infinity. The LHR now sends both (*,G) joins and (S,G) RPT prune messages towards the RP.

To configure a group to never follow the SPT, create the necessary prefix lists, then configure SPT switchover for the prefix-list.

Example

- The following example is to configure a group to never follow the SPT, create the necessary prefixlists, then configure SPT switchover for the spt-range prefix-list:

```
admin@Xorplus# set routing prefix-list IPv4 spt-range seq 1 permit prefix 235.0.0.0/8 ge 32
admin@Xorplus# set routing prefix-list IPv4 spt-range seq 1 permit prefix 238.0.0.0/8 ge 32
admin@Xorplus# set protocols pim spt-switchover infinity-and-beyond prefix-list spt-range
admin@Xorplus# commit
```

set protocols pim ssm prefix-list

The **set protocols pim ssm prefix-list** command sets a range of group addresses via a prefix-list that forces pim to never do SM over.

Command Syntax

set protocols pim [vrf<*vrf-name*>] ssm prefix-list <*prefix-list*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].
prefix-list <*prefix-list*>	Specifies the prefix-list name. The value is a string which has been set by comannd set routing prefix-list.

Example

- Configure a range of group addresses via a prefix-list.

```
admin@Xorplus# set protocols pim ssm prefix-list PreLst1
admin@Xorplus# set routing prefix-list ipv4-family PreLst1 permit prefix 233.0.0.0/8
admin@Xorplus# set routing prefix-list ipv4-family PreLst1 permit prefix 232.0.0.0/8
admin@Xorplus# commit
```

run show pim interface

The **run show pim interface** command shows information about all interfaces on which PIM-SM is enabled.

Command Syntax

run show pim interface [**detail**]

Example

- Show information about all interfaces on which PIM-SM is enabled.

```
admin@Xorplus# run show pim interface
Interface      State        Address    PIM Nbrs     PIM DR       FHR      IfChannels
----------   --------   ------   --------   --------   ----   ---------
loopback    up      1.1.1.1    0           local        0        0
vlan100        up           10.0.0.11  1           10.0.0.21    0        4
```

run show pim rp-info

The **run show igmp rp-info** command displays RP information for all the multicast groups.

Command Syntax
run show igmp rp-info

Parameter

None.

Example
• Display RP information for all the multicast groups.

```
admin@Xorplus# run show pim rp-info
RP address       group/prefix-list   OIF              I am RP    Source
3.3.3.3          224.1.1.1/32        vlan4094         no        Static
3.3.3.3          230.1.1.1/32        vlan4094         no        Static
3.3.3.3          231.1.1.1/32        vlan4094         no        Static
```

run show pim neighbor

The **run show pim neighbor** command shows information about PIM neighbors.

Command Syntax

run show pim neighbor

Example

- Show information about PIM neighbors.

```
admin@Xorplus# run show pim neighbor
Interface    Neighbor    Uptime       Holdtime     DR Pri
----------  ----------  ----------  ----------  ----------
vlan20       20.0.0.2     105          84           1
```

run show pim upstream

The **run show pim upstream** command displays upstream information about a S,G mroute.

Command Syntax

run show pim upstream

Example

- Show the upstream information about a S,G mroute.

```
admin@Xorplus# run show pim upstream
Iif Source       Group     State Uptime   JoinTimer RSTimer KATimer  RefCnt
br0 172.16.5.105 239.1.1.1 Prune 00:07:40 --:--:-- 00:00:36 00:02:50 1
!
```

run show mroute

The **run show igmp mroute** command displays the PIM routing table information.

Command Syntax
run show igmp mroute [**vrf** <*vrf-name*>]

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies a VRF name. The value is a string. It's a user-defined VRF set by the command **set ip vrf** <*vrf-name*> [**description** <*string*>].

Example

- Display the PIM routing table.

```
admin@XorPlus# run show mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set

Source          Group           Flags   Proto  Input            Output           TTL  Uptime
71.1.1.100      231.1.1.1       SFP             none   vlan771          none             0    --:--:--
81.1.1.100      231.1.1.1       SCT             IGMP   vlan4000         vlan771          1    00:03:57
```

mtrace

The **mtrace** command displays multicast traceroute towards specified IPv4 source and group address.

Command Syntax

- From the ">" prompt, use the following format,

mtrace source <*ipv4-src-addr*> [**group** <*ipv4-group-addr*>]

- From the "#" prompt, add **run** in front of the command,

run mtrace source <*ipv4-src-addr*> [**group** <*ipv4-group-addr*>]

Parameters

Parameter	Description
source <*ipv4-src-addr*>	Specifies the source IPv4 address to trace.
group <*ipv4-group-addr*>	Optional. Specifies the group IPv4 address to trace.

Example

- The following example traces with multicast source:

```
admin@PICOS> mtrace source 1.1.1.100
* Mtrace from 1.1.1.100 to 3.3.3.30 via group 0.0.0.0
Querying full reverse path...
 * switching to hop-by-hop:
  0  ? (3.3.3.30)
 -1  ? (3.3.3.3) PIM thresh^ 1
Round trip time 3 ms; total ttl of 1 required.
```

- The following example traces with multicast source and group address:

```
admin@PICOS# run mtrace source 1.1.1.100 group 224.1.1.1
* Mtrace from 1.1.1.100 to 3.3.3.30 via group 224.1.1.1
Querying full reverse path...
 * switching to hop-by-hop:
  0  ? (3.3.3.30)
 -1  ? (3.3.3.3) PIM (S,G) thresh^ 1
Round trip time 3 ms; total ttl of 1 required.
```

In the display result, "0" represents the switch currently executing mtrace, "-1" represents the first hop starting from the current switch and its interface IP address is 3.3.3.3.

run show pim group-type

The **run show pim group-type** command display SSM group ranges.

Command Syntax

None.

Example

- This example shows how to display information about PIM group ranges:

```
admin@Xorplus# run show pim group-type
SSM group range : 232.0.0.0/8
```

Multicast Source Discovery Protocol (MSDP) Commands

- set protocols msdp mesh-group source
- set protocols msdp mesh-group member
- run show msdp mesh-group
- run show msdp peer
- run show msdp sa

set protocols msdp mesh-group source

The **set protocols msdp mesh-group source** command is used to configure the source address of MSDP peers.

Command Syntax

set protocols msdp mesh-group < *mesh-group-name*> **source** <*source-address*>

Parameter

Parameter	Description
mesh-group < *mesh-group-name*>	Specifies the name of the MSDP mesh group. The value is a string.
source <*source-address*>	Specifies the address of the local RP device as the source address of the local MSDP device. The value is in dotted decimal format.

Usage Guidelines

Only one mesh group is allowed in one PIM-SM domain.

When configuring MSDP peers, configure the local MSDP device as the source and all the other remote MSDP peer devices in the same mesh group as members.

Example

- Create an MSDP mesh group.

```
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 member 3.3.3.3
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 source 2.2.2.2
admin@Xorplus# commit
```

set protocols msdp mesh-group member

The **set protocols msdp mesh-group member** command is used to configure the MSDP member devices.

Command Syntax

set protocols msdp mesh-group < *mesh-group-name*> **member** <*peer-address*>

Parameter

Parameter	Description
mesh-group < *mesh-group-name*>	Specifies the name of the MSDP mesh group. The value is a string.
member <*peer-address*>	Specifies the address of the remote MSDP peer that becomes a MSDP member. The value is in dotted decimal format.

Usage Guidelines

Only one mesh group is allowed in a PIM-SM domain.

When configuring MSDP peers, configure the local MSDP device as the source and all the other remote MSDP peer devices in the same mesh group as members.

Example

- Create an MSDP mesh group.

```
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 member 3.3.3.3
admin@Xorplus# set protocols msdp mesh-group 6.6.6.6 source 2.2.2.2
admin@Xorplus# commit
```

run show msdp mesh-group

The **run show msdp mesh-group** command displays the establishment state of MSDP peers.

Note: Use this command only on MSDP peers.

Command Syntax

run show msdp mesh-group

Parameter

Null.

Example

- View the establishment state of MSDP peers.

```
admin@Xorplus# run show msdp mesh-group
Mesh group : 6.6.6.6
  Source : 2.2.2.2
  Member         State
  3.3.3.3          established
```

run show msdp peer

The **run show msdp peer** command displays the status information of the MSDP peers.

Note: Use this command only on MSDP peers.

Command Syntax

run show msdp peer [*<peer-ip>* | **detail**]

Parameter

Parameter	Description
<peer-ip>	Optional. Specifies the address of a remote MSDP peer. If this parameter is not specified, information about all the MSDP peers will be displayed. The address is in dotted decimal notation.
detail	Optional. Displays detail information about the status of MSDP peers.

Example

- View the brief information about all the remote MSDP peers.

```
admin@Xorplus# run show msdp peer
Peer                      Local        State    Uptime   SaCnt
3.3.3.3                 2.2.2.2  established  06:10:45       2
```

- View the detail information about all the remote MSDP peers.

```
admin@Xorplus# run show msdp peer detail
Peer : 3.3.3.3
  Local               : 2.2.2.2
  Mesh Group          : 6.6.6.6
  State               : established
  Uptime              : 06:10:52
  Keepalive Timer     : 00:00:08
  Conn Retry Timer    : --:--:--
  Hold Timer          : 00:00:46
  Last Reset          : -
  Conn Attempts       : 22
  Established Changes : 1
  SA Count            : 2
  Statistics          :
                       Sent       Rcvd
    Keepalives :        371          4
    SAs        :          0        748
```

- View the detail information about a specific remote MSDP peer.

```
admin@Xorplus# run show msdp peer 3.3.3.3
Peer : 3.3.3.3
  Local               : 2.2.2.2
  Mesh Group          : 6.6.6.6
  State               : established
  Uptime              : 06:11:03
  Keepalive Timer     : 00:00:57
  Conn Retry Timer    : --:--:--
  Hold Timer          : 00:00:35
  Last Reset          : -
  Conn Attempts       : 22
  Established Changes : 1
  SA Count            : 2
```

```
Statistics          :
                     Sent       Rcvd
  Keepalives :        372          4
  SAs        :          0        748
```

run show msdp sa

The **run show msdp sa** command displays the (S, G) entries cached on MSDP peers.

Note: Use this command only on MSDP peers.

Command Syntax

run show msdp sa [**ip** <*ip-address*> | **detail**]

Parameter

Parameter	Description
ip <*ip-address*>	Optional. Specifies the address of a multicast source. If this parameter is not specified, (S, G) entries from all the multicast sources will be displayed. The address is in dotted decimal notation.
detail	Optional. Displays detail information about (S, G) entries cached on the device.

Example

- View the brief information about all (S, G) entries cached on the device.

```
admin@Xorplus# run show msdp sa
Source               Group            RP      Local  SPT  Uptime
200.200.200.2         237.0.0.2          3.3.3.3      n    y  00:15:17
200.200.200.2         237.0.0.3          3.3.3.3      n    y  00:13:35
```

- View the detail information about all (S, G) entries cached on the device.

```
admin@Xorplus# run show msdp sa detail
SA : (200.200.200.2,237.0.0.1)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
  Local       : no
  SPT Setup   : yes
  Uptime      : 05:27:01
  State Timer : 00:02:34

SA : (200.200.200.2,239.255.255.250)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
  Local       : no
  SPT Setup   : yes
  Uptime      : 06:04:55
  State Timer : 00:02:34
```

- View the detail (S, G) entries information of a specific multicast source cached on the device.

```
admin@Xorplus# run show msdp sa ip 200.200.200.2
SA : (200.200.200.2,237.0.0.1)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
  Local       : no
  SPT Setup   : yes
  Uptime      : 05:27:33
  State Timer : 00:03:02

SA : (200.200.200.2,239.255.255.250)
  RP          : 3.3.3.3
  Peer        : 3.3.3.3
```

```
Local       : no
SPT Setup   : yes
Uptime      : 06:05:27
State Timer : 00:03:02
```

Multicast VLAN Registration (MVR) Commands

- run show igmp-snooping mvr mvlan
- run show igmp-snooping mvr receiver-vlan
- set protocols igmp-snooping vlan-id mvr receiver vlan-list
- set protocols igmp-snooping vlan-id mvr source group

run show igmp-snooping mvr mvlan

The **run show igmp-snooping mvr mvlan** command is used to view MVLAN information.

Command Syntax

run show igmp-snooping mvr mvlan <*vlan id*>

Parameter

Parameter	Description
<*vlan-id*>	The VLAN ID of the given MVLAN

Example

- View MVR interface information.

```
admin@PICOS# run show ipmp-snooping mvr mvlan 100
Mvlan     Receiver-vlan
--------  ---------------
100        101, 102, 103
```

run show igmp-snooping mvr receiver-vlan

The **run show igmp-snooping mvr receiver-vlan** command shows information of the given receiver VLAN ID.

Command Syntax

run show igmp-snooping mvr receiver-vlan <*vlan-id*>

Parameter

Parameter	Description
<*vlan-id*>	The VLAN ID of the given receiver VLAN.

Example

- View the brief information of the MVRP receiver VLAN.

```
admin@PICOS# run show igmp-snooping mvr receiver-vlan 101
Receiver-vlan   Mvlan
-------------  --------------
101             100
```

set protocols igmp-snooping vlan-id mvr receiver vlan-list

The **set protocols igmp-snooping vlan-id mvr receiver vlan-list** command configure the MVR mapped VLAN IDs on the access ports.

The **delete protocols igmp-snooping vlan-id mvr receiver vlan-list** command deletes the configuration.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **mvr receiver vlan-list** <*vlan-range-string*>

delete protocols igmp-snooping vlan-id <*vlan-id*> **mvr receiver vlan-list**

Parameters

Parameter	Description
<*vlan-id*>	The multicast MVR VLAN ID.
<*vlan-range-string*>	The mapped receiver VLAN list for the given MVLAN.

Usage Guidelines

The IGMP query packets and stream traffic from the upstream port is updated to different VLAN ID in the vlan-list of the above configuration command. On the reverse direction, the IGMP report packets with the VLAN ID in the vlan-list are translated to the MVLAN accordingly.

The upstream traffic will go the trunk ports which have the VLAN ID as MVLAN.

Example

- Configure the receiver VLAN range as 101-199 for MVLAN 100.

```
admin@PICOS# set protocols igmp-snooping vlan-id 100 mvr receiver vlan-list 101-199
admin@PICOS# commit
```

set protocols igmp-snooping vlan-id mvr source group

The **set protocols igmp-snooping vlan-id mvr source group** command can be used to configure the source multicast group of a given MVLAN.

The **delete protocols igmp-snooping vlan-id mvr source group** command deletes the configuration.

Command Syntax

set protocols igmp-snooping vlan-id <*vlan-id*> **mvr source group** <*multicast-network-address*>/<*prefix-length*>

delete protocols igmp-snooping vlan-id <*vlan-id*> **mvr source group** <*multicast-network-address*>/<*prefix-length*>

Parameters

Parameter	Description
<*vlan-id*>	The MVLAN ID of the MVR multicast traffic from upstream.
<*multicast-network-address*>	The multicast group address of the MVR mapping.
<*prefix-length*>	The prefix length of the group address.

Usage Guidelines

Multiple source groups could be configured with one MVR VLAN instance.

Group overlapping is not allowed when configuring multiple MVLANs.

Example

- Configure the multicast source group range 225.0.0.1/8 for the given MVLAN 100.

```
admin@PICOS# set protocols igmp-snooping vlan-id 100 mvr source group 225.0.0.1/8
admin@PICOS# commit
```

OpenFlow Commands in CrossFlow Mode

To use the hybrid mode of the Openflow switch, enable the xovs mode in XorPlus system. Next, configure the interfaces to be used in XorPlus system. Then, exit to Linux system to add the flows required.

Commands

set xovs enable ***<true | false>***

set interface gigabit-ethernet ge-1/1/1 crossflow enable true

set interface gigabit-ethernet ge-1/1/1 crossflow local-control false

set vlans vlan-id ***<vlan-id>***

delete xovs

set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk

set interface gigabit-ethernet ge-1/1/1 family ethernet-switching vlan members ***<vlan-id>***

VXLAN Commands

- vxlans source-interface address
- vxlans udp-port
- set vxlans vni <text> decapsulation mode
- vxlans vni <text> encapsulation mode
- vxlans vni <text> encapsulation vlan
- vxlans vni <text> flood vtep
- vxlans vni <text> flood vtep <ipv4-addr> mac-address
- vxlans vni <text> flood vtep <ipv4-addr> traffic-type
- set vxlans vni vlan
- set vxlans tunnel-mac-leaning disable
- OVSDB VTEP command
  - set protocols ovsdb controller <controller-name> address
  - set protocols ovsdb controller <controller-name> inactivity-probe-duration 30000
  - set protocols ovsdb controller <controller-name> maximum-backoff-duration
  - set protocols ovsdb controller <controller-name> port
  - set protocols ovsdb controller c1 protocol
  - set protocols ovsdb interface
  - set protocols ovsdb management-ip
  - set protocols ovsdb ssl bootstrap
  - set protocols ovsdb ssl ca-cert
    - set protocols ovsdb ssl certificate
  - set protocols ovsdb ssl private-key
  - set vxlans ovsdb-managed
  - set protocols ovsdb controller vrf mgmt-vrf
- set vxlans l3-vni prefix-routes-only
- set vxlans l3-vni
- set vxlans vni mcast-group
- run show vxlan statistics
- run clear vxlan statistics
- run show vxlan vni
- run show vxlan address-table

vxlans source-interface address

User can configure vxlan source interface ip address .

Command Syntax

set vxlans source-interface <*interface*> address <*ipv4-addr*>

delete vxlans source-interface <*interface*> address <*ipv4-addr*>

Parameter
•<*interface*> The vlan interface, e.g. loopback or vlan10
•<*ipv4-addr*>The IPv4 address

Example
• This example demonstrates how to configure the vxlan to use the IP address 10.10.10.1 as the source address in the encapsulation fields of outbound VXLAN frames.

```
XorPlus# set vxlans source-interface loopback address 10.10.10.1
XorPlus# commit
```

vxlans udp-port

To configure the UDP destination port number for VXLAN, use the **set vxlans udp-port** command in L2/L3 configuration mode. The default VXLAN UDP port number is 4789.

Command Syntax

set vxlans udp-port *number*

Parameters

number	VXLAN UDP port number. The range of values is from 1024 to 65535.

Example

This example demonstrates how to configure the VXLAN UDP port association to 5000:

```
admin@XorPlus# set vxlans udp-port 5000
```

set vxlans vni <text> decapsulation mode

User can configure decapsulation mode for vxlan vni.

> **NOTE:**
> Trident3 platform switches do not support the following VXLAN commands:
>
> **set vxlans vni** <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-add**
>
> **set vxlans vni** <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-add-delete**
>
> **set vxlans vni** <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-add-replace**
>
> **set vxlans vni** <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-delete**
>
> **set vxlans vni** <*text*> **decapsulation mode** <*decapsulation-mode*> **service-vlan-replace**

Command Syntax
set vxlans vni <*text*> decapsulation mode <*decapsulation-mode*>

Parameter
• <*text*> VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted format 100.100.200
• <*decapsulation-mode*> Configure vxlan tunnel encapsulation mode. Required selection include:

- **none**: Nothing will change, untagged packets will stay untagged, tagged packets will stay tagged.
- **service-vlan-add**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port & vlan, the vlan id of the tag been added will be that vlan, otherwise will be PVID of that port.
- **service-vlan-add-delete**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port & vlan, the vlan id of the tag been added will be that vlan. Otherwise, it will be PVID of that port. From access to access, delete tag for tagged packets.
- **service-vlan-add-replace**: From network ports to access ports, add 802.1Q tag for both untagged/tagged packets. If the access port is matched by port & vlan, the vlan id of the tag been added will be that vlan, otherwise will be PVID of that port. From access to access, replace tag for tagged packets. This is default value.
- **service-vlan-delete**: From access to access, delete tag for tagged packets.
- **service-vlan-replace**: From access to access, replace tag for tagged packets.
- **service-vlan-per-port**: The decapsulated packet can be tagged or untagged dynamically based on the setting on the output port.

Example
• This example demonstrates how to configure the VXLAN tunnel decapsulation mode for the VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 decapsulation mode none
admin@XorPlus# commit
```

vxlans vni <text> encapsulation mode

User can configure encapsulation mode for vxlan vni.

> **NOTE:**
> Trident3 platform switches do not support the following VXLAN commands:
>
> **set vxlans vni** <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-add**
>
> **set vxlans vni** <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-add-delete**
>
> **set vxlans vni** <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-add-replace**
>
> **set vxlans vni** <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-delete**
>
> **set vxlans vni** <*text*> **encapsulation mode** <*decapsulation-mode*> **service-vlan-replace**

Command Syntax
set vxlans vni <*text*> encapsulation mode <*encapsulation-mode*>

Parameter
• <*text*> VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted format 100.100.200
• <*encapsulation-mode*> Configure vxlan tunnel encapsulation mode. Required select include:

- **none**: Nothing will change, untagged packets will stay untagged, tagged packets will stay tagged.
- **service-vlan-add**: Add 802.1Q tag for untagged packets, and nothing changed with tagged packets. Encapsulation vlan is required.
- **service-vlan-add-delete**: Add 802.1Q tag for untagged packets, and delete tag for tagged packets. Encapsulation vlan is required.
- **service-vlan-add-replace**: Add 802.1Q tag for untagged packets, and replace tag for tagged packets. Encapsulation vlan is required.
- **service-vlan-delete**: Delete 802.1Q tag for tagged packets, and nothing changed with untagged packets. This is default value according to RFC 7348.
- **service-vlan-replace**: Replace vlan id of 802.1Q tag for tagged packets, and nothing changed with untagged packets. Encapsulation vlan is required

Example
• This example demonstrates how to configure the VXLAN tunnel encapsulation mode for the VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 encapsulation mode none
admin@XorPlus# commit
```

vxlans vni <text> encapsulation vlan

User can configure flood vtep address for vxlan vni.

Command Syntax
set vxlans vni <*text*> encapsulation vlan <*vlan-id*>

Parameter
• <*text*> VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
• <*vlan-id*> Add vlan id for vxlan tunnel encapsulation mode. Required select include:

Example
• This example demonstrates how to configure the VXLAN tunnel encapsulation mode add vlan id for the VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 encapsulation vlan 100
admin@XorPlus# commit
```

vxlans vni <text> flood vtep

User can configure flood vtep address for vxlan vni.

Command Syntax
set vxlans vni <*text*> flood vtep <*ipv4-addr*>

Parameter
• <*text*> VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
• <*ipv4-addr*> IPv4 address of vxlan vtep.

Example
• This example demonstrates how to configure the VXLAN head-end replication flood lists for the VNI 10010.

```
XorPlus# set vxlans vni 10010 flood vtep 20.20.20.1
XorPlus# set vxlans vni 10010 flood vtep 30.30.30.1
XorPlus# commit
```

vxlans vni <text> flood vtep <ipv4-addr> mac-address

User can configure the flood vtep address set static mac address for vni.

Command Syntax
set vxlans vni <*text*> flood vtep <*ipv4-addr*> mac-address <*macaddr*>

delete vxlans vni <*text*> flood vtep <*ipv4-addr*> mac-address <*macaddr*>

Parameter
• <*text*> VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
• <*ipv4-addr*> IPv4 address of vxlan vtep.
• < *macaddr*> Static mac address identifier

Example
• This example demonstrates how to configure the VXLAN flood vtep address set static mac address is 00:e0:fc:00:0a:0b for the VNI

```
XorPlus# set vxlans vni 10010 flood vtep 20.20.20.1 mac-address 00:e0:fc:00:0a:0b
XorPlus# commit
```

vxlans vni <text> flood vtep <ipv4-addr> traffic-type

User can configure the flood vtep address set forwarding traffic type for vni .

Command Syntax
set vxlans vni <*text*> flood vtep <*ipv4-addr*> traffic-type < *type-mode* >

delete vxlans vni <*text*> flood vtep <*ipv4-addr*> *traffic-type*

Parameter
• <*text*> VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
• <*ipv4-addr*> IPv4 address of vxlan vtep.
• <*type-mode*> Forwarding traffic type mode. Required select include:

- **BUM** Transport BUM(broadcast, unknow unicast and multicast) traffic only
- **all** Transport all traffic through this vtep, the default mode
- **unicast** Transport known unicast traffic only

Example

• This example demonstrates how to configure the VXLAN flood vtep address set forwarding traffic type is BUM for the VNI 10010

```
XorPlus# set vxlans vni 10010 flood vtep 20.20.20.1 traffic-type BUM
XorPlus# commit
```

set vxlans vni vlan

User can configure mapping between VLAN to VXLAN VNI. Note that, there is a one-to-one mapping between a VXLAN VNI and a VLAN.

Command Syntax

set vxlans vni <*text*> **vlan** <*vlan-id*>

delete vxlans vni <*text*> **vlan** <*vlan-id*>

Parameter
• <*text*> VXLAN segment ID, decimal format ranges 1-16777215 or notation dotted foramt 100.100.200
• <*vlan-id*> VLAN tag identifier, the valid VLAN numbers range 1-4094.

Example
• This example demonstrates how to configure mapping between VLAN 100 to VXLAN VNI 10010.

```
admin@XorPlus# set vxlans vni 10010 vlan 100
admin@XorPlus# commit
```

set vxlans tunnel-mac-leaning disable

User can configure disable VXLAN tunnels interface mac learning.

Command Syntax
set vxlans tunnel-mac-leaning disable <*boolean*>

delete set vxlans tunnel-mac-leaning disable

Parameter
•<*boolean*> enable or disable VXLAN tunnels interface mac learning.

- **true** disable VXLAN tunnels interface mac learning
- **false** enable VXLAN tunnels interfaces mac learning

Example
• This example demonstrates how to configure disable VXLAN tunnels interface mac learning.

```
admin@XorPlus# set vxlans tunnel-mac-leaning disable true
admin@XorPlus# commit
```

OVSDB VTEP command

- set protocols ovsdb controller <controller-name> address
- set protocols ovsdb controller <controller-name> inactivity-probe-duration 30000
- set protocols ovsdb controller <controller-name> maximum-backoff-duration
- set protocols ovsdb controller <controller-name> port
- set protocols ovsdb controller c1 protocol
- set protocols ovsdb interface
- set protocols ovsdb management-ip
- set protocols ovsdb ssl bootstrap
- set protocols ovsdb ssl ca-cert
  - set protocols ovsdb ssl certificate
- set protocols ovsdb ssl private-key
- set vxlans ovsdb-managed
- set protocols ovsdb controller vrf mgmt-vrf

set protocols ovsdb controller <controller-name> address

User can configure ovsdb vtep to establish an active OVSDB tcp/ssl connection to a controller .

Command Syntax
set protocols ovsdb controller <controller-name> address <*ip-addr*>

delete protocols ovsdb controller <controller-name> address

Parameter

- <*controller-name*> controller name.
- <*ip-address*> Specifies the destination IPv4/IPv6 address for the tcp/ssl connection.

Example
• This example demonstrates how to configure a tcp/ssl connection to port 6632 at 10.10.50.220.

```
admin@XorPlus# set protocols ovsdb controller c1 address 10.10.50.220
admin@XorPlus# commit
```

set protocols ovsdb controller <controller-name> inactivity-probe-duration 30000

User can configure ovsdb vtep tcp/ssl connection inactivity probe duration.

Command Syntax
set protocols ovsdb controller <*controller-name*> inactivity-probe-duration <*uint*>

delete protocols ovsdb controller <*controller-name*> inactivity-probe-duration

Parameter

- <*controller-name*> controller name.
- <*uint*> Number of milliseconds the connection can be inactive before an inactivity probe is sent.

Example
• This example demonstrates how to configure a tcp/ssl connection inactivity probe duration.

```
admin@XorPlus# set protocols ovsdb controller c1 inactivity-probe-duration 30001
admin@XorPlus# commit
```

set protocols ovsdb controller <controller-name> maximum-backoff-duration

User can configure ovsdb vtep tcp/ssl connection maximum backoff duration.

Command Syntax
set protocols ovsdb controller <*controller-name*> maximum-backoff-duration <*uint*>

delete protocols ovsdb controller <*controller-name*> maximum-backoff-duration

Parameter

- <*controller-name*> controller name.
- <*uint*> Number of milliseconds OVSDB server waits before it re-attempts to connect with an controller, the valid VLAN numbers range 1000-4294967295.

Example
• This example demonstrates how to configure a tcp/ssl connection maximum backoff duration.

```
admin@XorPlus# set protocols ovsdb controller c1 maximum-backoff-duration 1001
admin@XorPlus# commit
```

set protocols ovsdb controller <controller-name> port

User can configure ovsdb vtep tcp/ssl connection port number.

Command Syntax
set protocols ovsdb controller <*controller-name*> port <*port-number*>

delete protocols ovsdb controller <*controller-name*> port

Parameter

- <*controller-name*> controller name.
- <*port-number*> Specifies the destination port or listen port for the tcp/ssl connection. The value range for the port-number argument is 0 to 65535. .

Example
This example demonstrates how to configure an tcp/ssl connection port.

```
admin@XorPlus# set protocols ovsdb controller c1 port 6632
admin@XorPlus# commit
```

set protocols ovsdb controller c1 protocol

User can configure ovsdb vtep establish connection with protocol.

Command Syntax
set protocols ovsdb controller *<controller-name>* protocol *<protocol-mode>*

delete protocols ovsdb controller *<controller-name>* protocol

Parameter

- *<controller-name>* controller name.
- *<protocol-mode>* Configure establish an OVSDB SSL or TCP connection with a one controller or listen for OVSDB SSL or TCP connection requests:
  - **pssl** Listening for SSL connection requests from controllers
  - **ptcp** Listening for TCP connection requests from controllers
  - **ssl** Establishing an active SSL connection to a controller
  - **tcp** Establishing an active TCP connection to a controller

Example
This example demonstrates how to configure ovsdb vtep establish connection protocol with ptcp

```
admin@XorPlus# set protocols ovsdb controller c1 protocol ptcp
admin@XorPlus# commit
```

set protocols ovsdb interface

User can configure ovsdb vtep access port.
Command Syntax
set protocols ovsdb interface <*port*>

delete protocols ovsdb interface

Parameter
• <*port*> port identifier,the valid ports range 1-52.

Example
• This example demonstrates how to configure specify te-1/1/1 as a ovsdb vtep access port.

```
admin@XorPlus# set protocols ovsdb interface te-1/1/1
admin@XorPlus# commit
```

set protocols ovsdb management-ip

User can configure ovsdb vtep access port.

Command Syntax
set protocols ovsdb management-ip *<ipv4/ipv6>*

delete protocols ovsdb management-ip

Parameter
• *<ipv4/ipv6>* ipv4 or ipv6 address, configuring the OVSDB VTEP's management IP for controller .

Example
• This example demonstrates how to configure the VTEP's management IP.

```
admin@XorPlus# set protocols ovsdb management-ip 10.10.51.157
admin@XorPlus# commit
```

set protocols ovsdb ssl bootstrap

User can configure obtain the CA certificate from the SSL peer.
Command Syntax
set protocols ovsdb SSL bootstrap <*boolean*>

delete protocols ovsdb ssl bootstrap

Parameter
•<*boolean*>enable or disable ssl bootstrap.

- **true** enable ssl bootstrap, the ca certificate automatically downloaded from ssl peer.
- **false** disable ssl bootstrap, the ca certificate manually copy to the /ovs/var/lib/openvswitch/pki directory

Example
• This example demonstrates how to configure ovsdb ssl bootstrap.

```
admin@XorPlus# set protocols ovsdb SSL bootstrap true
admin@XorPlus# commit
```

set protocols ovsdb ssl ca-cert

User can configure CA certificate file for ssl connected.
Command Syntax
set protocols ovsdb ssl ca-cert *<file>*

delete protocols ovsdb ssl ca-cert

Parameter
•*<file>* Specifies ssl connect with CA certificate file name.

Example
• This example demonstrates how to configure CA certificate file name for ssl connected.

```
admin@XorPlus# set protocols ovsdb ssl ca-cert "/ovs/var/lib/openvswitch/pki/controller.cacert"
admin@XorPlus# commit
```

- set protocols ovsdb ssl certificate

set protocols ovsdb ssl certificate

User can configure certificate file for ssl connected.
Command Syntax
set protocols ovsdb SSL certificate *<file>*

delete protocols ovsdb ssl certificate

Parameter
•*<file>* Specifies ssl connect with certificate file name.

Example
• This example configure certificate file name for ssl connected.

```
admin@XorPlus# set protocols ovsdb ssl certificate "/ovs/var/lib/openvswitch/pki/pica8-cert.pem"
admin@XorPlus# commit
```

set protocols ovsdb ssl private-key

User can configure a private key file for ssl connected.
Command Syntax
set protocols ovsdb ssl private-key *<file>*

delete protocols ovsdb ssl private-key

Parameter
•*<file>* Specifies ssl connect with private key file name.

Example
• This example demonstrates how to configure private key file name for ssl connected.

```
admin@XorPlus# set protocols ovsdb ssl private-key "/ovs/var/lib/openvswitch/pki/pica8-privkey.pem"
admin@XorPlus# commit
```

set vxlans ovsdb-managed

User can configure enable vxlan ovsdb managed.

Command Syntax
set vxlans ovsdb-managed <*boolean*>

delete vxlans ovsdb-managed

Parameter
•<*boolean*>enable or disable vxlan ovsdb managed.

- **true** enable vxlan ovsdb managed
- **false** disable vxlan ovsdb managed

Example
• This example demonstrates how to configure enable vxlan ovsdb managed.

```
admin@XorPlus# set vxlans ovsdb-managed true
admin@XorPlus# commit
```

set protocols ovsdb controller vrf mgmt-vrf

The **set protocols ovsdb controller vrf mgmt-vrf** command configures to run the Open vSwitch Database (OVSDB) management protocol in the management VRF.

Command Syntax

set protocols ovsdb controller <*controller-name*> **vrf mgmt-vrf**

Parameter

Parameter	Description
controller <*controller-name*>	Specifies the OVSDB controller name. The value is a string.

Usage Guidelines

OVSDB management protocol runs in the default VRF by default, and supports to be configured in the management VRF. The corresponding OVSDB controller is required to be route reachable in the VRF running OVSDB management protocol.

Note: The latest configuration overrides the previous one.

Example

- Configure the OVSDB management protocol to run in the management VRF.

```
admin@Xorplus# set protocols ovsdb controller c1 vrf mgmt-vrf
admin@Xorplus# commit
```

set vxlans l3-vni prefix-routes-only

Run the command **set vxlans l3-vni prefix-routes-only** to advertise the prefix routes only. Without this command prefix routes wont be advertised to the peer devices.

Note that this configuration its mandatory in asymmetric EVPN routing model where we want to advertise the Type-5 prefix routes. In symmetric EVPN routing model however, we will use the command **set vxlans l3-vni** <vni-id> to advertise host routes as Type-2 advertisements and Type-5 prefix routes.

Command Syntax

set vxlans vrf <*vrf-name*> **l3-vni** <*vni-id*> **prefix-routes-only**

delete vxlans vrf <*vrf-name*> **l3-vni** <*vni-id*> **prefix-routes-only**

Parameters

vrf <*vrf-name*>	Optional, specifies the VRF name.
l3-vni <*vni-id*>	Specifies the layer 3 VNI ID.

Example

This example demonstrates how to enable prefix routes only advertisement as Type-5 routes for a given VRF.

```
admin@XorPlus# set vxlans vrf vrf1 l3-vni 100 prefix-routes-only
```

set vxlans l3-vni

The command **set vxlans l3-vni** is used to add the L3 VNI ID to VXLAN routing. It will advertise the Type-2 host advertisements and Type-5 prefix routes for the VNI. The optional argument **prefix-routes-only** can be added to the command to advertise the prefix routes only. This configuration is used in EVPN Asymmetric routing to sync external routes between devices.

Run the command **delete vxlans l3-vni** to remove this configuration from the system.

Command Syntax

set vxlans [vrf <*vrf-name***>] l3-vni <***vni-id***> [prefix-routes-only]**

delete vxlans [vrf <*vrf-name***>] l3-vni <***vni-id***> [prefix-routes-only]**

Parameters

vrf <*vrf-name*>	Optional, specifies the VRF name.
l3-vni <*vni-id*>	Specifies the layer 3 VNI ID.

Example

This example demonstrates how to enable advertisement of Type-2 and Type-5 routes for a given VRF and VNI ID.

```
admin@XorPlus# set vxlans vrf vrf1 l3-vni 100
```

set vxlans vni mcast-group

The **set vxlans vni mcast-group** command is used to enable the multicast replication function of BUM message and to configure the multicast replication address of VNI.

> **NOTE:**
> PICOS supports only one VXLAN segment mapping to one IP multicast group, which is the way to provide the optimal multicast forwarding. That is, to have multiple VXLAN segments share a single IP multicast group in the core network is not supported.

Command Syntax

set vxlans vni <*vni-id*> **mcast-group** <*ip-address*>

delete vxlans vni <*vni-id*> **mcast-group** <*ip-address*>

Parameters

Parameter	Description
vni <*vni-id*>	Specifies the layer 3 VNI ID.
mcast-group <*ip-address*>	Specifies the multicast replication address.

Example

- This example enables the multicast replication function.

```
admin@XorPlus# set vxlans vni 1 mcast-group  1.1.1.1
```

run show vxlan statistics

The **run show vxlan statistics** command shows traffic statistics of the VXLAN tunnel.

Command Syntax

run show vxlan statistics [**vni** <*vni-id*>]

Parameter

Parameter	Description
vni <*vni-id*>	Optional. Specifies VXLAN VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200. If VNI ID is specified, it will only show the statistics of the specified VXLAN tunnel. If VNI ID is not specified, it will show the statistics of all the VXLAN tunnels.

Example

- Show traffic statistics of the VXLAN tunnel.

```
admin@Xorplus# run show vxlan statistics
VNID     Interface    Vlan ID  Type       Input(Pkts)           Output(Pkts)        Input(Octets)         Output(Oc
-------- ------------ ------- ----------- -------------------- -------------------- -------------------- ----------
9991001   ae10        1000     Access     413                  401                  26504                 828
9991002   te-1/1/5    1000     Access     2335                 3022                 149440                204468
```

run clear vxlan statistics

The **run clear vxlan statistics** command clears traffic statistics of the VXLAN tunnel.

Command Syntax

run clear vxlan statistics [**vni** <*vni-id*>]

Parameter

Parameter	Description
vni <*vni-id*>	Optional. Specifies VXLAN VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200.

Usage Guidelines

If you want to obtain the latest statistics information, use this command to clear the past statistics information. When new packets coming, new statistics information is generated.

Example

- Clear traffic statistics of the VXLAN tunnel.

```
admin@Xorplus# run clear vxlan statistics
admin@Xorplus# commit
```

run show vxlan vni

Run the command **run show vxlan vni** to list all interfaces, their types and the associated egress and VLAN IDs for a specific VNI. Interface types includes Access, Network (unicast) and Network (multicast).

Example:

```
admin@SVNE2# run show vxlan vni 10030
Interface      ID             Type           Egress     Vlan ID
-----------    -----------    -----------    -------    --------
ae1            0x80000004     Access         100012     30
ae2            0x80000005     Access         100013     30
te-1/1/9       0x80000006     Access         100014     30
te-1/1/17      0x80000007     Network(UC)    200258
te-1/1/17      0x80000009     Network(MC)    100020
te-1/1/17      0x8000000a     Network(UC)    200258
te-1/1/17      0x8000000c     Network(MC)    100022
te-1/1/19      0x8000000d     Network(UC)    100017
te-1/1/19      0x8000000f     Network(MC)    100024
```

run show vxlan address-table

Run the command **run show vxlan address-table** to display the VXLAN address table on the switch. MAC addresses belonging to different VNI's are listed along with its type, interface and the associated VTEP.

Example:

```
admin@SVNE3# run show vxlan address-table
VNID           MAC address          Type       Interface          VTEP
-----------    -----------------    -------    ----------------    ---------------
99             04:f8:f8:20:67:7b    Dynamic                         10.226.14.254
99             18:5a:58:37:55:e1    Dynamic                         10.226.14.253
99             50:9a:4c:e6:7e:71    Dynamic                         10.226.14.201
10020          00:1e:c9:bb:c0:3c    Dynamic    ge-1/1/19
10020          04:f8:f8:20:67:7b    Dynamic                         10.226.14.254
10020          18:5a:58:37:55:e1    Dynamic                         10.226.14.253
10020          50:9a:4c:e6:7e:71    Dynamic                         10.226.14.201
10030          04:f8:f8:20:67:7b    Dynamic                         10.226.14.254
10030          18:5a:58:37:55:e1    Dynamic                         10.226.14.253
10030          22:00:00:00:00:00    Dynamic                         10.226.14.254
10030          50:9a:4c:e6:7e:71    Dynamic                         10.226.14.201
Entries in access port:  1
Entries in network port: 10
```

BGP EVPN Commands

- run show bgp evpn route
- run show bgp evpn summary
- run show bgp evpn vni
- run show evpn es
- run show evpn mac vni
- set interface aggregate-ethernet evpn mh es-df-pref
- set interface aggregate-ethernet evpn mh es-id
- set interface aggregate-ethernet evpn mh es-sys-mac
- set l3-interface routed-interface router-mac
- set l3-interface vlan-interface anycast address
- set l3-interface vlan-interface anycast mac
- set l3-interface vlan-interface router-mac
- set protocols bgp evpn advertise-all-vni
- set protocols bgp evpn advertise-default-gw
- set protocols bgp evpn advertise ipv4-unicast
- set protocols bgp evpn advertise ipv6-unicast
- set protocols bgp evpn advertise-svi-ip
- set protocols bgp evpn default-originate
- set protocols bgp evpn disable-ead-evi-rx
- set protocols bgp evpn disable-ead-evi-tx
- set protocols bgp evpn vni
- set protocols bgp evpn vni advertise-default-gw
- set protocols bgp evpn vni advertise-subnet
- set protocols bgp evpn vni advertise-svi-ip
- set protocols bgp evpn vni rd
- set protocols bgp evpn vni route-target type
- set protocols bgp neighbor evpn activate
- set protocols bgp neighbor evpn allowas-in
- set protocols bgp neighbor evpn route-map
- set protocols bgp neighbor evpn route-reflector-client
- set protocols bgp vrf evpn advertise-pip ip
- set protocols evpn mh mac-holdtime
- set protocols evpn mh neigh-holdtime
- set protocols evpn mh redirect-off
- set protocols evpn mh startup-delay
- set vxlans vni arp-nd-suppress disable

run show bgp evpn route

Run the command **run show bgp evpn route** to display all BGP EVPN routes in the routing table.

Command Syntax

run show bgp evpn route

Example

- Display all BGP EVPN routes.

```
admin@51.134# run show bgp evpn route
   Network          Next Hop            Metric LocPrf Weight Path
                    Extended Community
Route Distinguisher: 134.134.134.134:2
*> [5]:[0]:[24]:[33.1.1.0]
                    134.134.134.134          0         32768 i
                    ET:8 RT:134:9999 Rmac:04:f8:f8:20:6c:7b
Route Distinguisher: 134.134.134.134:3
*> [3]:[0]:[32]:[134.134.134.134]
                    134.134.134.134                    32768 i
                    ET:8 RT:134:22221
Route Distinguisher: 134.134.134.134:4
*> [3]:[0]:[32]:[134.134.134.134]
                    134.134.134.134                    32768 i
                    ET:8 RT:134:22222
Route Distinguisher: 134.134.134.134:5
*> [3]:[0]:[32]:[134.134.134.134]
                    134.134.134.134                    32768 i
                    ET:8 RT:134:33333
Route Distinguisher: 201.201.201.201:2
*> [5]:[0]:[24]:[22.1.1.0]
                    201.201.201.201          0             0 201 i
                    RT:201:9999 ET:8 Rmac:c4:39:3a:fb:be:d9
Route Distinguisher: 201.201.201.201:3
*> [2]:[0]:[48]:[00:11:11:11:11:11]
                    201.201.201.201                       0 201 i
                    RT:201:9999 RT:201:22221 ET:8 Rmac:c4:39:3a:fb:be:d9
*> [2]:[0]:[48]:[00:11:11:11:11:11]:[32]:[21.1.1.1]
                    201.201.201.201                       0 201 i
                    RT:201:9999 RT:201:22221 ET:8 Rmac:c4:39:3a:fb:be:d9
*> [3]:[0]:[32]:[201.201.201.201]
                    201.201.201.201                       0 201 i
                    RT:201:22221 ET:8
Route Distinguisher: 201.201.201.201:4
*> [3]:[0]:[32]:[201.201.201.201]
                    201.201.201.201                       0 201 i
                    RT:201:22222 ET:8
```

run show bgp evpn summary

Run the command **run show bgp evpn summary** to display some basic information related to BGP EVPN. The output includes BGP router ID, local AS number, VRF membership and peer count etc. The output also includes a brief display of BGP EVPN packet statistics such as messages sent/received and router ID of remote peer.

Command Syntax

run show bgp evpn summary

Example

- Configure BGP EVPN to disable BUM traffic.

```
admin@Xorplus# run show bgp evpn summary
BGP router identifier 1.1.1.1, local AS number 65001 vrf-id 0
BGP table version 0
RIB entries 3, using 576 bytes of memory
Peers 1, using 21 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
2.2.2.2         4      65001         9         8        0    0    0 00:03:16            2

Total number of neighbors 1
```

run show bgp evpn vni

Run the command **run show bgp evpn vni** to display EVPN VNI related information. The output displays information such as VXLAN VNI gateway MAC-IP advertisement is enabled or not, SVI MAC-IP advertisement enabled or disabled. Also if advertisement of all VNIs is enabled or not. Other information displayed includes VNI ID, Type, RD, Import RT, Export RT and Tenant VRF.

Command Syntax

run show bgp evpn vni

Example

- Display BGP EVPN VNI information.

```
admin@Xorplus# run show bgp evpn vni
Advertise Gateway Macip: Disabled
Advertise SVI Macip: Disabled
Advertise All VNI flag: Enabled
BUM flooding: Head-end replication
Number of L2 VNIs: 1
Number of L3 VNIs: 0
Flags: * - Kernel
  VNI        Type RD                  Import RT              Export RT               Tenant VRF
* 10         L2   1.1.1.1:2           65001:10               65001:10               default
```

run show evpn es

The **run show evpn es** command is used to display the all the Ethernet segments configured on the device. It also displays the auto generated type-3 ESI for each segment, its type, the name of the LAG interface and the VTEPs involved.

Example:

```
admin@ACC2# run show evpn es
Type: B bypass, L local, R remote, N non-DF
ESI                               Type      ES-IF                 VTEPs
03:00:22:22:22:22:22:00:00:01      LR        ae1                  10.226.14.253,10.226.14.254
03:00:22:22:22:22:22:00:00:02      LR        ae2                  10.226.14.253,10.226.14.254
```

To check the detailed information of the Ethernet segments, add the optional keyword detail at the end of the command as shown below.

```
admin@ACC2# run show evpn es detail
ESI: 03:00:22:22:22:22:22:00:00:01
 Type: Local,Remote
 Interface: ae1
 State: up
 Bridge port: yes
 Ready for BGP: yes
 VNI Count: 2
 MAC Count: 0
 DF status: df
 DF preference: 32767
 Nexthop group: 536870913
 VTEPs:
     10.226.14.253 df_alg: preference df_pref: 32767 nh: 268435459
     10.226.14.254 df_alg: preference df_pref: 32767 nh: 268435460


ESI: 03:00:22:22:22:22:22:00:00:02
 Type: Local,Remote
 Interface: ae2
 State: up
 Bridge port: yes
 Ready for BGP: yes
 VNI Count: 2
 MAC Count: 0
 DF status: df
 DF preference: 32767
 Nexthop group: 536870914
 VTEPs:
     10.226.14.253 df_alg: preference df_pref: 32767 nh: 268435459
     10.226.14.254 df_alg: preference df_pref: 32767 nh: 268435460
```

run show evpn mac vni

Run the command **run show evpn mac vni** to display all the MAC addresses learned on different interfaces belonging to a particular VNI. It also shows whether the MAC is learned locally or remotely and shows the associated VLAN.

Example:

```
admin@SVNE3# run show evpn mac vni 10030
Number of MACs (local and remote) known for this VNI: 5
Flags: N=sync-neighs, I=local-inactive, P=peer-active, X=peer-proxy
MAC               Type   Flags Intf/Remote ES/VTEP            VLAN  Seq #'s
22:00:00:00:00:00 remote       10.226.14.254                       0/0
18:5a:58:37:55:e1 remote       10.226.14.253                       0/0
50:9a:4c:e6:7e:71 remote       10.226.14.201                       0/0
18:5a:58:37:64:61 local        vlan30                        30    0/0
04:f8:f8:20:67:7b remote       10.226.14.254                       0/0
```

set interface aggregate-ethernet evpn mh es-df-pref

Run the command **set interface aggregate-ethernet evpn mh es-df-pref** to set the preference value used in the Designated Forwarder (DF) election process on a given aggregate Ethernet interface. The default value of DF preference is 32767. If there is a tie between the nodes over the preference value then the VTEP with the smallest IP address wins the election.

Please note that DF preference can only be set for an aggregate Ethernet interface.

Run the command **delete interface aggregate-ethernet evpn mh es-df-pref** to remove this configuration from the switch.

Command Syntax

set interface aggregate-ethernet <*interface*> **evpn mh es-df-pref <***preference***>**

delete interface aggregate-ethernet <*interface*> **evpn mh es-df-pref**

Parameter

Parameter	Description
aggregate-ethernet <*interface*>	Specifies the aggregate Ethernet interface, the value is a string, e.g. ae1.
es-df-pref <*preference***>**	Specifies the Ethernet segment DF preference, the value is an integer that ranges from 1 to 65535. The default value is 32767.

Example

- Configure the DF preference value to 45000.

```
admin@Xorplus# set interface aggregate-ethernet ae1 evpn mh es-df-pref 45000
admin@Xorplus# commit
```

set interface aggregate-ethernet evpn mh es-id

Run the command **set interface aggregate-ethernet evpn mh es-id** to set the Ethernet Segment Identifier (ES-ID) for the EVPN multi-homing feature on a given aggregate Ethernet interface.

Run the command **delete interface aggregate-ethernet evpn mh es-id** to delete the ES-ID from the switch configuration.

Command Syntax

set interface aggregate-ethernet <*aggregate-ethernet*> **evpn mh es-id <***ES-ID***>**

delete interface aggregate-ethernet <*aggregate-ethernet***> evpn mh es-id <***ES-ID***>**

Parameter

Parameter	Description
aggregate-ethernet <*aggregate-ethernet*>	Specifies the aggregate Ethernet interface, the value is a string, e.g. ae1.
es-id <*ES-ID*>	Specifies the ES-ID. The value is an integer that ranges from 1 to 16777215.

Example

- Configure the ES-ID to 40 for aggregate Ethernet interface ae1.

```
admin@Xorplus# set interface aggregate-ethernet ae1 evpn mh es-id 40
admin@Xorplus# commit
```

set interface aggregate-ethernet evpn mh es-sys-mac

Run the command **set interface aggregate-ethernet evpn mh es-sys-mac** to configure the EVPN multi-homing Ethernet Segment System MAC address on a given aggregate Ethernet interface.

Run the command **delete set interface aggregate-ethernet evpn mh es-sys-mac** to delete this configuration from the switch.

Command Syntax

set interface aggregate-ethernet <*aggregate-ethernet*> **evpn mh es-sys-mac <***system-mac***>**

delete interface aggregate-ethernet <*aggregate-ethernet*> **evpn mh es-sys-mac <***system-mac***>**

Parameter

Parameter	Description
aggregate-ethernet <*aggregate-ethernet*>	Specifies the aggregate Ethernet interface, the value is a string, e.g. ae1.
es-sys-mac <*system-mac***>**	Specifies the Ethernet segment system MAC address, the value is in 48 bit hexadecimal MAC address format, e.g. 00:22:22:22:22:22

Example

- Configure the EVPN multi-homing Ethernet segment system MAC for interface ae1.

```
admin@Xorplus# set interface aggregate-ethernet ae1 evpn mh es-sys-mac 00:22:22:22:22:22
admin@Xorplus# commit
```

set l3-interface routed-interface router-mac

The **set l3-interface routed-interface router-mac** command sets the router MAC address of the anycast gateway on a routed interface or sub-interface.

Command Syntax

set l3-interface routed-interface <*interface-name*> **router-mac** <*macaddr*>

Parameter

Parameter	Description
routed-interface <*interface-name*>	Specifies a routed interface name or sub-interface name. The value is a string.
router-mac <*macaddr*>	Specifies the virtual MAC address of anycast gateway. The value is a string in xx:xx:xx:xx:xx:xx format where *x* is a hexadecimal number.

Example

- Configure the router MAC address of the anycast gateway on a routed interface.

```
admin@Xorplus# set l3-interface routed-interface rif-te3 router-mac 00:00:10:00:00:FE
admin@Xorplus# commit
```

set l3-interface vlan-interface anycast address

The **set l3-interface vlan-interface anycast address** command configures the virtual IP address of the anycast gateway.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **anycast address** <*ip-address*> **prefix-length** <*prefix*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies the L3 VLAN interface. The value is a string.
address <*ip-address*>	Specifies IPv4 or IPv6 address.
prefix-length <*prefix*>	Specifies the network prefix length. The range is 4-32 for IPv4 addresses, and 1-128 for IPv6 addresses.

Usage Guidelines

Follow the rules below when configuring the anycast IPv4 / IPv6 address:

- For IPv4, the anycast IPv4 address and the VLAN interface IPv4 address should be configured in the same network segment to ensure that the MLAG pair can work normally.
- For IPv6, the anycast IPv6 address and the global IPv6 address of the VLAN interface should be configured in the same network segment to ensure that the MLAG pair can work normally.
- Anycast IP address list on both devices of MLAG pair must be the same.

Example

- Configure the virtual IP address of the anycast gateway.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast address 10.0.1.1 prefix-length 24
admin@Xorplus# commit
```

set l3-interface vlan-interface anycast mac

The **set l3-interface vlan-interface anycast mac** command configures the virtual MAC address of the anycast gateway.

Command Syntax

set l3-interface vlan-interface <*interface-name*> **anycast mac** <*mac-address*>

Parameter

Parameter	Description
vlan-interface <*interface-name*>	Specifies the L3 VLAN interface. The value is a string.
mac <*mac-address*>	Specifies the virtual MAC address of anycast gateway. The value is a string in xx:xx:xx:xx:xx:xx format where *x* is a hexadecimal number.

Example

- Configure the virtual MAC address of the anycast gateway.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 anycast mac AE:00:10:00:00:FE
admin@Xorplus# commit
```

set l3-interface vlan-interface router-mac

The **set l3-interface vlan-interface router-mac** command configures the router MAC address of the anycast gateway.

Command Syntax

set l3-interface vlan-interface <*vlan-interface-name*> **router-mac** <*macaddr*>

Parameter

Parameter	Description
vlan-interface <*vlan-interface-name*>	Specifies the L3 VLAN interface. The value is a string.
router-mac <*macaddr*>	Specifies the virtual MAC address of anycast gateway. The value is a string in xx:xx:xx:xx:xx:xx format where *x* is a hexadecimal number.

Example

- Configure the router MAC address of the anycast gateway.

```
admin@Xorplus# set l3-interface vlan-interface vlan10 router-mac 00:00:10:00:00:FE
admin@Xorplus# commit
```

set protocols bgp evpn advertise-all-vni

The **set protocols bgp evpn advertise-all-vni** command is used to enable the BGP control plane for all VNIs configured on the switch in the default VRF.

Note that only leaf switches that are VTEPs need this configuration.

The **delete protocols bgp evpn advertise-all-vni** command can be used to delete this configuration.

Command Syntax

set protocols bgp evpn advertise-all-vni

delete protocols bgp evpn advertise-all-vni

Example

- Configure BGP EVPN to advertise all VNIs in the default VRF.

```
admin@Xorplus# set protocols bgp evpn advertise-all-vni
admin@Xorplus# commit
```

set protocols bgp evpn advertise-default-gw

The **set protocols bgp evpn advertise-default-gw** command is used to configure the gateway VTEPs to advertise the IP/MAC address. Optional parameter **vrf** can be added to identify the VRF for which to advertise the IP/MAC address.

The **delete protocols bgp evpn advertise-default-gw** can be used to delete the configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn advertise-default-gw**

delete protocols bgp [vrf <*vrf-name*>**] evpn advertise-default-gw**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.

Example

- Configure BGP EVPN to advertise default gateway for VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn advertise-default-gw
admin@Xorplus# commit
```

set protocols bgp evpn advertise ipv4-unicast

The **set protocols bgp evpn advertise ipv4-unicast** command is used to announce IPv4 prefixes in the BGP RIB as EVPN Type-5 routes. Add the optional parameter **route-map** if you want to add a route map filter to the IPv4 Type-5 route advertisement. If the route map filter is not used, all the IPv4 routes in the BGP RIB are included in the advertisement. Optional parameter **vrf** can be used if you want the command to take effect on a specific VRF.

The **delete protocols bgp evpn advertise ipv4-unicast** command can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn advertise ipv4-unicast [route-map** <*route-map*>**]**

delete protocols bgp [vrf <*vrf-name***>] evpn advertise ipv4-unicast [route-map** <*route-map*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF name. The value is a string.
route-map <*route-map*>	Optional. Specifies the route-map to filter the Type-5 IPv4 routes while advertising. The value is a string.

Example

- Configure the device to announce the IPv4 prefixes in VRF BLUE for EVPN and apply the map1 route-map filter.

```
admin@Xorplus# set protocols bgp vrf BLUE advertise ipv4-unicast route-map map1
admin@Xorplus# commit
```

set protocols bgp evpn advertise ipv6-unicast

The command **set protocols bgp evpn advertise ipv6-unicast** is used to configure the device to announce IPv6 prefixes in the BGP RIB as EVPN Type-5 routes. Add the optional parameter **route-map** if you want to add a route map filter to the IPv6 Type-5 route advertisement. If the route map filter is not used, all the IPv6 routes in the BGP RIB are included in the advertisement. The other optional parameters are **vrf** to specify a VRF for this command to take effect on.

To delete this configuration, run the command **delete set protocols bgp evpn advertise ipv6-unicast.**

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn advertise ipv6-unicast [route-map** <*route-map*>**]**

delete protocols bgp [vrf <*vrf-name***>] evpn advertise ipv6-unicast [route-map** <*route-map*>**]**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
route-map <*route-map*>	Specifies a route map filter for the IPv6 Type-5 route advertisement. The value is a string.

Example

- Configure the device to advertise EVPN Type-5 IPv6 routes in VRF BLUE and apply route-map map1.

```
admin@Xorplus# set protocols bgp vrf BLUE advertise ipv6-unicast route-map map1
admin@Xorplus# commit
```

set protocols bgp evpn advertise-svi-ip

Run the command **set protocols bgp evpn advertise-svi-ip** to advertise the local SVI IP address so that it can be accessible from remote VTEPs. This command is needed when unique SVIs are used across different racks. You should not use this command if SVI addresses are reused across different racks and are not unique.

Run the command **delete protocols bgp evpn advertise-svi-ip** to remove this configuration.

Command Syntax

set protocols bgp evpn advertise-svi-ip

delete protocols bgp evpn advertise-svi-ip

Example

- Configure the device to advertise the local SVI IP.

```
admin@Xorplus# set protocols bgp evpn advertise-svi-ip
admin@Xorplus# commit
```

set protocols bgp evpn default-originate

To enable originating a default Type-5 route, run the command **set protocols bgp evpn default-originate**. Both the IPv4 and IPv6 default Type-5 routes are supported to be originated. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

The command **delete protocols bgp evpn default-originate** can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name***>] evpn default-originate** <**ipv4 | ipv6>**

delete protocols bgp [vrf <*vrf-name*>**] evpn default-originate <ipv4 | ipv6**>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
default-originate <ipv4|ipv6>	Specifies whether IPv4 or IPv6 Type-5 route to be originated.

Example

- Configure the device to originate the IPv4 default Type-5 routes for VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn default-originate ipv4
admin@Xorplus# commit
```

set protocols bgp evpn disable-ead-evi-rx

Some implementations of EVPN do not advertise EAD-per-EVI routes so to be compatible with these vendors; we need to manually disable advertisement of EAD-per-EVI routes. To activate the VTEP upon receiving EAD-per-ES route and suppress the dependency on EAD-per-EVI routes, run the command **set protocols bgp evpn disable-ead-evi-rx.**

Optional parameter **vrf** can be used to identify a specific VRF for this command to take effect on.

The command **delete protocols bgp evpn disable-ead-evi-rx** can be used to remove this configuration.

Command Syntax

set protocol bgp [vrf <*vrf-name***>] evpn disable-ead-evi-rx**

delete protocol bgp [vrf <*vrf-name***>] evpn disable-ead-evi-rx**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.

Example

- Configure the device to disable EVPN advertisement of EAD-per-EVI routes in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn disable-ead-evi-rx
admin@Xorplus# commit
```

set protocols bgp evpn disable-ead-evi-tx

Since the Type-1/EAD (Ethernet Auto Discovery) routes are to be advertised in the following two ways as per RFC 7432:

1. Ethernet Auto Discovery per Ethernet Segment (EAD-per-ES) routes
2. Ethernet Auto Discovery per EVPN Instance (EAD-per-EVI) routes

Some implementations of EVPN don't advertise EAD-per-EVI routes so to be compatible with these vendors; we need to manually disable advertisement of EAD-per-EVI routes. To suppress the advertisement of EAD-per-EVI routes, run the command **set protocols bgp evpn disable-ead-evi-tx.** Optional parameter **vrf** can be used to identify a specific VRF for this command to take effect on.

To delete this configuration, run the command **delete protocols bgp evpn disable-ead-evi-tx.**

Command Syntax

set protocols bgp [vrf <*vrf-name***>] evpn disable-ead-evi-tx**

delete protocols bgp [vrf <*vrf-name***>] evpn disable-ead-evi-tx**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.

Example

- Configure the device to disable EVPN advertisement of EAD-per-EVI routes in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn disable-ead-evi-tx
admin@Xorplus# commit
```

set protocols bgp evpn vni

To add a VXLAN VNI to BGP EVPN routing, run the command **set protocols bgp evpn vni**. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

The command **delete protocols bgp evpn vni** can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*>

delete protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
vni <*vni*>	Specifies the VNI to add to the BGP EVPN routing. The value is an integer that ranges from 1 to 16777215.

Example

- Configure the device to add VNI 20 to EVPN BGP routing in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn vni 20
admin@Xorplus# commit
```

set protocols bgp evpn vni advertise-default-gw

Run the command **set protocols bgp evpn vni advertise-default-gw** to configure the gateway VTEPs to advertise their IP/MAC routes for the specified VNI. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

Run the command **delete protocols bgp evpn vni advertise-default-gw** to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*> **advertise-default-gw**

delete protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*> **advertise-default-gw**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
vni <*vni*>	Specifies the VNI for which to advertise the default gateway.

Example

- Configure the device to advertise the default gateway in VRF BLUE for VNI 20.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn vni 20 advertise-default-gw
admin@Xorplus# commit
```

set protocols bgp evpn vni advertise-subnet

Run the command **set protocols bgp evpn vni advertise-subnet** to advertise the subnet corresponding to the specified VNI. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

Run the command **delete protocols bgp evpn vni advertise-subnet** to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*> **advertise-subnet**

delete protocols bgp [vrf <*vrf-name*>**] evpn vni** <*vni*> **advertise-subnet**

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies the name of the VRF. The value is a string.
vni <*vni*>	Specifies the VNI, its value is an integer that ranges from 1 to 16777215.

Example

- Configure the device to advertise the locally attached subnet corresponding to VNI 20 in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn vni 20 advertise-subnet
admin@Xorplus# commit
```

set protocols bgp evpn vni advertise-svi-ip

To advertise the local SVI IP address behind a specific VNI, run the command **set protocols bgp evpn vni advertise-svi-ip**.

To delete the configuration, run the command **delete protocols bgp evpn vni advertise-svi-ip.**

Command Syntax

set protocols bgp evpn vni <*vni*> **advertise-svi-ip**

delete protocols bgp evpn vni <*vni*> **advertise-svi-ip**

Parameter

Parameter	Description
vni <*vni*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.

Example

- Configure the device to advertise the local SVI IP behind VNI 20.

```
admin@Xorplus# set protocols bgp evpn vni 20 advertise-svi-ip
admin@Xorplus# commit
```

set protocols bgp evpn vni rd

Run the command **set protocols bgp evpn vni rd** if you do not want that route distinguisher (RD) to be automatically derived and define them manually.

Run the command **delete protocols bgp evpn vni rd** to delete this configuration.

Command Syntax

set protocols bgp evpn vni <*vni-id*> **rd** <*rd*>

delete protocol bgp evpn vni <*vni-id*> **rd** <*rd*>

Parameter

Parameter	Description
vni <*vni-id*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.
rd <*rd*>	Specifies the route distinguisher. The value follows the format *RouterID:VNI-Index.*

Usage Guidelines

When the switch learns about a local VNI and there is no configuration available in the system regarding this VNI then the import and export route targets (RTs) and route distinguisher (RD) for this VNI will be automatically calculated. The RTs are automatically derived as *AS:VNI*, whereas RD is derived as *Router-ID:VNI-Index.*

For Type-2 and Type-3 routes coming from the layer 2 VNI, the RD is calculated as *VXLAN-local0-tunnelip:VNI* instead of *Router-ID:VNI.* Since EVPN routes may have the same MAC and/or the IP address; RDs are used to remove ambiguity in such cases. RTs are used to identify the VPN membership of routes.

Example

- Configure RD for VNI 20.

```
admin@Xorplus#  set protocols bgp evpn vni 20 rd 10.1.1.1:20
admin@Xorplus# commit
```

set protocols bgp evpn vni route-target type

If we want the route target (RT) to be configured manually instead of being auto-configured, run the command **set protocols bgp evpn vni route-target type.** The command specifies the route target and its type as well. Parameter **type** can have three possible values, **export**, **import** or **both**. If you choose **both** then the RT can be used as both an import and export route target.

Run the command **delete protocols bgp evpn vni route-target** to delete this configuration.

Command Syntax

set protocols bgp evpn vni <*vni-id*> **route-target** <*route-target*> **type <both | export | import>**

delete protocols bgp evpn vni <*vni-id*> **route-target** <route-target> **type <both | export | import>**

Parameter

Parameter	Description
vni <*vni-id*>	Specifies the VNI ID. The value is an integer that ranges from 1 to 16777215.
route-target <*route-target*>	Specifies the route target. The value of route target follows the format *AS:VNI,* e.g. 65100:20
type <both | export | import>	Specifies the RT type as either import, export or both.

Example

- Configure the route target value 65100:20 for VNI 20 and apply this RT for both export and import of routes.

```
admin@Xorplus# set protocols bgp evpn vni 20 route-target 65100:20 type both
admin@Xorplus# commit
```

set protocols bgp neighbor evpn activate

Run the command **set protocols bgp neighbor evpn activate** to enable or disable the BGP peer within the EVPN address family to enable EVPN route exchange with the specified BGP peer.

Optional parameter **vrf** can be used to identify a VRF, if not defined, the command takes effect on the default VRF.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn activate <true | false>**

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
activate <true | false>	Enables or disables the address family for the specified neighbor • **true:** Enables the address family for the specified neighbor. • **false:** Disables the address family for the specified neighbor.

Example

- Configure the device to enable EVPN BGP route exchange with peer 3.3.3.3 in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn activate true
admin@Xorplus# commit
```

set protocols bgp neighbor evpn allowas-in

To allow BGP route updates from peers with the same AS number as the current system AS; run the command **set protocol bgp neighbor evpn allowas-in**. This configuration is needed when different BGP peers reside in different locations that cannot be directly connected but they both use the same AS number. Parameter **vrf** is optional and if not specified then the command will affect the default VRF.

The parameter value **<1-10>** configures the number of accepted occurrences of the current system AS number in AS path.

The parameter **origin** configures BGP to only accept routes originated with the same AS number as that of the current system.

Run the command **delete protocols bgp neighbor evpn allowas-in** to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn allowas-in {**<1-10> | **origin}**

delete protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn allowas-in {**<1-10> | **origin}**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
allowas-in {<1-10> | **origin}**	Value <**1-10>** specifies the number of occurrences of AS in AS path, **origin** configures BGP to only accept routes originated with the same AS number as that of the system.

Example

- Configure BGP to accept BGP EVPN route updates from peer 3.3.3.3 in VRF BLUE and also the accepted routes originated with the same AS number as the system.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn allowas-in origin
admin@Xorplus# commit
```

set protocols bgp neighbor evpn route-map

Run the command **set protocols bgp neighbor evpn route-map** to configure an inbound or outbound route map for an EVPN neighbor. The parameter value of neighbor is the BGP neighbor for which to specify the route map. The value of parameter route-map is where you specify the name of the route map to apply and keywords **in** or **out** are to specify whether the route map applies to inbound or outbound traffic. Optional parameter **vrf** can be used to specify a VRF. If VRF is not specified then the command applies to the default VRF.

The command **delete protocols bgp neighbor evpn route-map** can be used to remove this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn {in | out} route-map** <*route-map*>

delete protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn {in | out} route-map** <*route-map*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.
in|out	Keywords to specify the inbound or outbound direction for route map.
route-map <*route-map*>	Specifies the name of the route map.

Example

- Configure to apply route map *map1* to for EVPN BGP peer 3.3.3.3 in the inbound direction for the VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn in route-map map1
admin@Xorplus# commit
```

set protocols bgp neighbor evpn route-reflector-client

Run the command **set protocols bgp neighbor evpn route-reflector-client** to configure the BGP node to act as a route reflector for the specified BGP peer for EVPN. Optional parameter **vrf** can be used to specify a VRF, if no VRF is specified the command takes effect on the default VRF.

The command **delete protocols bgp neighbor evpn route-reflector-client** can be used to delete this configuration.

Command Syntax

set protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn route-reflector-client**

delete protocols bgp [vrf <*vrf-name*>**] {neighbor** <*ip*>**| peer-group** <*peer-group*> **|interface** <*interface*>**} evpn route-reflector-client**

Parameter

Parameter	Description
vrf <*vrf-name*>	Optional. Specifies the name of the VRF. The value is a string.
neighbor <*ip*>	Specifies the IPv4/IPv6 address of a peer.
peer-group <*peer-group*>	Specifies a peer group.
interface <*interface*>	Specifies an L3 interface for BGP connection. The value could be a VLAN interface name, loopback interface name, routed interface or sub-interface name.

Example

- Configure the BGP to act as route reflector for the specified BGP peer for EVPN in VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE neighbor 3.3.3.3 evpn route-reflector-client
admin@Xorplus# commit
```

set protocols bgp vrf evpn advertise-pip ip

Run the command **set protocols bgp vrf evpn advertise-pip ip** to advertise the Primary IP Address (PIP) for a given VRF. Parameter **vrf** is optional and if not defined then the command takes effects on the default VRF. We can specify a specific IP address to advertise by adding **ip** <*ipv4*>.

The **delete protocols bgp vrf evpn advertise-pip ip** can be used to delete this configuration.

Command Syntax

set protocols bgp vrf <*vrf-name*> **evpn advertise-pip ip** <*ipv4*>

delete protocols bgp vrf <*vrf-name*> **evpn advertise-pip ip** <*ipv4*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies the name of the VRF. The value is a string.
ip <*ipv4*>	Specifies the IPv4 address to advertise. The value is a string in IPv4 dotted decimal format.

Example

- Configure BGP EVPN to advertise PIP 10.1.1.1 for VRF BLUE.

```
admin@Xorplus# set protocols bgp vrf BLUE evpn advertise-pip ip 10.1.1.1
admin@Xorplus# commit
```

set protocols evpn mh mac-holdtime

Run the command **set protocols evpn mh mac-holdtime** to configure the EVPN MH MAC hold time in seconds. This is the length of time for which a device maintains the SYNC MAC entries after the Ethernet segment (ES) peer's type-2 route is deleted. The device will try and attempt to establish reachability with MAC on the local ES during this time. The MAC hold time ranges from 0 to 86400 and the default value is 1080 seconds.

Run the command **delete protocols evpn mh mac-holdtime** to delete this configuration.

Note: This is a global configuration and affects the MH configuration on the whole device.

Command Syntax

set protocols evpn mh mac-holdtime <*seconds*>

delete protocols evpn mh mac-holdtime

Parameter

Parameter	Description
mac-holdtime <*seconds*>	Specifies the MAC hold time in seconds, the range is from 0 to 86400. The default value is 1080 seconds.

Example

- Configure the EVPN MH MAC hold time to 234 seconds.

```
admin@Xorplus# set protocols evpn mh mac-holdtime 234
admin@Xorplus# commit
```

set protocols evpn mh neigh-holdtime

Run the command **set protocols evpn mh neigh-holdtime** to configure the neighbor entry hold time in seconds. The device will maintain the SYNC neighbor entries during this time after the ES peer's EVPN type-2 route is deleted. The device independently tries to establish reachability with the MAC/host on the local ES during this time period.

Run the command **delete protocols evpn mh neigh-holdtime** to delete this configuration and revert back to the default value which is 1080 seconds.

Note: This is a global EVPN MH configuration and affects the whole device.

Command Syntax

set protocols evpn mh neigh-holdtime <*seconds*>

delete protocols evpn mh neigh-holdtime

Parameter

Parameter	Description
neigh-holdtime <*seconds*>	Specifies the neighbor entry hold time in seconds. The value ranges from 0 to 86400. The default value is 1080 seconds.

Example

- Configure the EVPN MH neighbor entry hold time to 234 seconds.

```
admin@Xorplus# set protocols evpn mh neigh-holdtime 234
admin@Xorplus# commit
```

set protocols evpn mh redirect-off

Run the command **set protocols evpn mh redirect-off** to disable fast failover of traffic destined to the access port via the VXLAN overlay.

Run the command **delete protocols evpn mh redirect-off** to remove this configuration and enable fast failover of traffic.

Note: This is a global configuration and affects the whole device.

Command Syntax

set protocols evpn mh redirect-off

delete protocols evpn mh redirect-off

Example

- Disable fast failover of traffic.

```
admin@Xorplus# set protocols evpn mh redirect-off
admin@Xorplus# commit
```

set protocols evpn mh startup-delay

Run the command **set protocols evpn mh startup-delay** to configure the duration of time for which the device keeps the EVPN multihoming LAG interfaces in protocol down state after a device reboot or process restart. This delays allows the VXLAN overlay to complete its initialization and helps in a smooth operation.

Run the command **delete protocols evpn mh startup-delay** to remove this configuration and revert to default which is 180 seconds.

Command Syntax

set protocols evpn mh startup-delay *<seconds>*

delete protocols evpn mh startup-delay

Parameter

Parameter	Description
startup-delay *<seconds>*	Specifies the startup-delay in seconds. The value ranges from 0 to 216000, the default value is 180 seconds.

Example

- Set the startup-delay to 200 seconds.

```
admin@Xorplus# set protocols evpn mh startup-delay 200
admin@Xorplus# commit
```

set vxlans vni arp-nd-suppress disable

The **set vxlans vni arp-nd-suppress disable** command is used to enable or disable ARP/ND suppression function in MP-BGP EVPN networks.

Command Syntax

set vxlans vni <*vni-id*> **arp-nd-suppress disable <true | false>**

Parameter

Parameter	Description
vni <*vni-id*>	Specifies the L2 VNI ID. The value is in decimal format with range of 1-16777215 or in dotted notation format such as 100.100.200.
disable <true | false>	Enable or disable ARP/ND suppression function. The value could be **true** or **false**. • **true**: Disable ARP/ND suppression. • **false**: Enable ARP/ND suppression. By default, ARP/ND suppression is disabled.

Example

- Enable ARP/ND suppression function.

```
admin@Xorplus# set vxlans vni 10010 arp-nd-suppress disable false
admin@Xorplus# commit
```

PoE Configuration Commands

Power over Ethernet (PoE) is a convenient way to deliver electrical power to network devices. Rather than running power over a separate electrical circuit, with PoE electrical power is carried over Ethernet cables, meaning only one cable connection is required to the device. Enabling PoE requires administrators to become familiar with a series of PoE commands. This page provides links to 11 of those commands. Follow the links to learn how to set max power thresholds, set PoE detection type, enable or disable PoE on a port-by-port basis, set the type of power limit on specific ports (PoE interface threshold mode), display PoE power status and more.

- set poe interface max-power
- set poe interface detection-type
- set poe interface enable
- set poe interface mode
- set poe interface priority
- set poe interface threshold-mode
- set poe power management-mode
- set poe power mode
- set poe interface lldp-negotiation
- set poe power voltage
- set protocols poe traceoptions flag all disable
- run show poe interface
- run show poe power

set poe interface max-power

NOTE:
This command is not available for S5810-48TS-P, S5860-24XB-U, S3410L-24TF-P, S3410C-16TMS-P, S3410C-16TF-P, S3410C-16TMS-P and S3410C-8TMS-P series switches:

- On **N3248PXE-ON**, all the RJ45 ports of the switch support UPoE. For these UPoE ports, the maximum output power is 99 watts.
- On **N3248P-ON**, all the RJ45 ports of the switch support PoE but not UPoE, the maximum output power of each port is 30 watts.
- On **N3224PX-ON**, all the RJ45 ports of the switch support UPoE. For these UPoE ports, the maximum output power is 99 watts.
- On **N3224P-ON**, all the RJ45 ports of the switch support PoE but not UPoE, the maximum output power of each port is 30 watts.
- On **S5860-24XB-U**, all the RJ45 ports of the switch support UPoE. For these UPoE ports, the maximum output power is 90 watts.
- On **S3410L-24TF-P**, all the RJ45 ports of the switch support PoE, the maximum output power of each port is 30 watts.
- On **S3410C-8TMS-P**, only the first eight RJ45 ports of the switch support PoE, the maximum output power of each port is 30 watts.

The **set poe interface max-power** command configures maximum output power of all the ports or a specific port.

Command Syntax

set poe interface {<*interface-name*> | **all**} **max-power** <*integer*>

Parameter

Parameter	Description
interface {< *interface-name* > | **all**}	Specifies interface name. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that sets a same maximum output power on all RJ45 ports.

max-power <*integer***>**	Specifies maximum output power of a port. The value is an integer, the unit is watt.
	• On **AS4610-30P** and **AS4610-54P**,
	  • Only the last 8 RJ45 ports of the switch, which are, ge-1/1/17 - ge-1/1/24 on AS4610-30P, ge-1/1/41 - ge-1/1/48 on AS4610-54P, support UPoE.
	  • For UPoE ports the range is from 1W to 51W, for other ports the range is from 1W to 32W. The default value is 16W.
	• On **AS4630-54NPE**/**AS4630-54PE**, the first 48 RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power can be set up to 90 watts, the default value is 30 watts.
	• On **AS4625-54P**, the 48 x 1G RJ45 ports on the front panel support PoE. Port1~Port40 support supports IEEE802.3at/af, the maximum output power supported is up to 30 watts, Port41~Port48 support IEEE802.3bt standard, the maximum output power supported is up to 90 watts.
	• On **S5860-24MG-U**, the 24 x 10G RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power can be set up to 90 watts.
	• On **S5860-48XMG-U**, the first 48 x 10G RJ45 ports on the front panel support PoE, only the first 24 x 10G RJ45 ports on the front panel support UPoE. For these UPoE ports, the maximum output power supported is up to 90 watts. For other PoE ports, the maximum output power supported is 30 watts.
	• On **S3410-24TS-P**, the 24 x 1G RJ45 ports on the front panel support PoE. For these PoE ports, the maximum output power can be set up to 30 watts.
	• On **S3410C-8TMS-P**, the 2 x 5G and first 6 x 1G RJ45 ports on the front panel support PoE. For these PoE ports, the maximum output power can be set up to 30 watts.

Usage Guidelines

Maximum output power configured on a specific port has a higher priority than that of global configuration. For example,

```
admin@Xorplus# set poe interface all max-power 20
admin@Xorplus# set poe interface ge-1/1/7 max-power 25
```

The result of the above configuration is: the maximum output power on ge-1/1/7 port is 25W, other ports are 20W.

NOTE:
- To make the set of max-power take effect, user need to disable and re-enable PoE function of the interface by using the **set poe interface {**<*port-id*> | **all} enable <true | false>** command.
- The max-power value should be at least 20% greater than the consumed power of the interface. We can use the **run show poe interface** {<*port-id*> | **all**} command to find the consume power.
- PoE over LLDP power negotiation takes a precedence over the max-power configured on the switch. If PoE over LLDP power negotiation function is enabled, the power value provided by PICA8 switch uses power over LLDP negotiation rather than the power value configured on the switch interface.

Example

- Set the maximum output power of port ge-1/1/7 to 30W.

```
admin@Xorplus# set poe interface ge-1/1/7 max-power 30
admin@Xorplus# commit
```

set poe interface detection-type

This command is applied on AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24MG-U, S5860-48XMG-U and S3410-24TS-P.

The **set poe interface detection-type** command configures PoE detection type of all the ports or a specific ethernet port.

Command Syntax

set poe interface {<*port-id*> | **all**} **detection-type** <*value*>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set a same detection type on all ports.
detection-type <*value*>	Specifies PoE detection type, the value is an integer that ranges from 0 to 5. 0: NO detection. 1: Legacy capacitive detection only. 2: IEEE 802.3af 4-Point detection only. 3: IEEE 802.3af 4-Point followed by legacy. 4: IEEE 802.3af 2-Point(not support). 5: IEEE 802.3af 2-Point followed by legacy. The default value is 3.

Note:

Configuration on a specific port has a higher priority than that of global configuration.

Example

This example is to configure PoE detection-type 5 on all the ports and ge-1/1/1:

```
admin@XorPlus# set poe interface all detection-type 5
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 detection-type 5
admin@XorPlus# commit
```

set poe interface enable

The **set poe interface enable** command enables PoE function on all ports or on a specific port.

Command Syntax

set poe interface {<*port-id*> | **all**} **enable** <**true | false**>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies port ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that enable or disable PoE on all ports.
enable <**true | false**>	Enable or disable PoE function. • **true**: enable PoE function. • **false**: disable PoE function. By default, PoE function is disabled.

Note:

Configuration on a specific port has a higher priority than that of global configuration. For example, if a specific port enables PoE function but the global configuration disables PoE function, then PoE function of all ports is disabled except this specific port.

Example
• This example is to enable PoE on all the ports and ge-1/1/1.

```
admin@XorPlus# set poe interface all enable true
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 enable true
admin@XorPlus# commit
```

set poe interface mode

This command is applied on AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24MG-U, S5860-48XMG-U and S3410-24TS-P.

The **set poe interface mode** command configures PoE pair mode on all the ports or a specific physical port.

Command Sytax

set poe interface {<*port-id*> | **all**} **mode** <*value*>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set a same mode on all ports.
mode <*value*>	Specifies PoE pair mode, the value can be **signal** and **spare**. • **signal**: Pair type A, deliver power with data transmit wires. • **spare**: Pair type B, deliver power with spare wires. The default value is signal.

Note:

Configuration on a specific port has a higher priority than that of global configuration.

Example

This example is to configure pair mode spare on all the ports and ge-1/1/1:

```
admin@XorPlus# set poe interface all mode spare
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 mode spare
admin@XorPlus# commit
```

set poe interface priority

The **set poe interface priority** command configures PoE priority on all the ports or on a specific ethernet port.

Command Syntax

On AS4610-30P, AS4610-54P, AS4630-54PE, S5810-48TS-P, S5860-24MG-U, S5860-48XMG-U, S3410L-24TF-P, S3410-24TS-P, and S3410C-8TMS-P:

set poe interface {*<port-id>* | **all**} **priority** <**critical | high | medium | low**>

On other PoE supported switches:

set poe interface {*<port-id>* | **all**} **priority** <**critical | high | low**>

Parameter

Parameter	Description
interface {*<port-id>* | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set all ports with a same PoE priority.
priority <**critical | high | medium | low**>	Specifies PoE priority. On AS4610-30P, AS4610-54P, AS4630-54PE, S5810-48TS-P, S5860-24MG-U, S5860-48XMG-U, S3410L-24TF-P, S3410-24TS-P, 3410C-16TMS-P, 3410C-16TF-P and S3410C-8TMS-P: The value is **critical**, **high**, **medium** and **low**. The priority is: critical > high > medium > low. The default value is medium. On other PoE supported switches: The value is **critical**, **high** and **low**. The priority is: critical > high > low. The default value is low.

Usage Guidlines

Configuration on a specific port has a higher priority than that of global configuration. For example, if the global configuration of PoE priority is set to high, while PoE priority on a specific port is set to critical, then PoE priority on this specific port is critical, other ports are high.

If a port is set as higher priority and a situation arises where there is not sufficient power for all the PoE ports, the available power is directed to the higher priority port(s). If the switch needs to shut down powered devices because a power supply fails and there is insufficient power, low priority devices are shut before high priority powered devices. Thus, security cameras, emergency phones, and other high priority devices should be set to a high priority.

Example

This example is to configure priority critical on all the ports and ge-1/1/1:

```
admin@XorPlus# set poe interface all priority critical
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 priority critical
admin@XorPlus# commit
```

set poe interface threshold-mode

This command is applied on AS4610-30P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24MG-U, S5860-48XMG-U and S3410-24TS-P.

The **set poe interface threshold-mode** configures PoE threshold-mode on all the ports or a specific physical port.

Command Syntax

set poe interface {<*port-id*> | **all**} **threshold-mode** <*value*>

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates a global configuration that set a same threshold mode on all ports.
threshold-mode <*value*>	The value is an interger that ranges from 0 to 2. 0: None (max power 16.2W) (Default). 1: Class Based (allows the port to draw up to advertised class max). 2: User defined (User-defined max power value), configured through max power threshold configuration command below. This command configures the type of power limit on the specific port. For the class-based power threshold, the class max power values are as follows: Class 0: 16.2W Class 1: 4.2W Class 2: 7.4W Class 3: 15W Class 4: 30W Class 5: 45W Class 6: 60W Class 7: 75W Class 8: 90W

Example

• This example is to configure threshold-mode 2 (user defined) on all the ports and ge-1/1/1.

```
admin@XorPlus# set poe interface all threshold-mode 2
admin@XorPlus# commit

admin@XorPlus# set poe interface ge-1/1/1 threshold-mode 2
admin@XorPlus# commit
```

set poe power management-mode

> This command is not available for S5810-48TS-P, S5860-24XB-U, S3410F-24TF-P,3410C-16TF-P, 3410C-16TMS-P, S3410C-8TMS-P, N32xx and N22xx series switches.

The **set poe power management-mode** command configures PoE power management-mode on all the ports or on a specific ethernet port.

Command Syntax

set poe power management-mode <*value*>

Parameter

<*value*>*:* The value is an integer that ranges from 1 to 4. The default value is 1.

1	Static Power Management with Port Priority
2	Dynamic Power Management with Port Priority
3	Static Power Management without Port Priority
4	Dynamic Power Management without Port Priority

1:

- When a PD is detected on a specific port, the PoE controller allows power on the port if available power is greater than the maximum power threshold configured on the port, and total allocated power is below the guard band.
- When the available power is less than the maximum power threshold configured on the port and the port priority is lower than the priority of all powered ports the PoE controller does not allow power on the port.
- When the available power is less than the maximum power threshold configured on the port and the port priority is greater than the priority of powered ports, the PoE controller disconnects low priority ports and allows the higher priority port to power up.

2:

- When a PD is detected on a specific port, the PoE controller allows power on the port if available power from the power source is greater than the maximum power threshold configured on the port and the total allocated power is below the guard band.
- When available power is less than the maximum power threshold configured on the port and port priority is less than the port priority set on all powered ports, the PoE controller does not allow power on the port.
- When available power is less than the maximum power threshold configured or the port and the port priority is greater than the priority of currently powered ports, the PoE controller disconnects the low priority ports and allows the port to power up.
- When the total consumed power exceeds the configured power limit of power source, low priority ports are turned off.

3:

- When a PD is detected on a specific port,the PoE controller allows power on the port if available power is greater than the maximum power threshold configured on the port, and total allocated power is below the guard band.
- When the available power is less than the maximum power threshold configured on the port, the PoE controller does not allow power on this port since port priority is not taken into effect, lower priority ports are not disconnected to power higher priority ports.

4:

- When a PD is detected on a specific port, the PoE controller allows power on the port if available power from the power source is greater than the maximum power threshold configured on the port and the total allocated power is below the guard band.
- When the total consumed power exceeds the configured power limit of power source, the PoE controller starts powering down the ports beginning with the highest port number.

Example

This example is to configure power management-mode to 1:

```
admin@XorPlus# set poe power management-mode 1
admin@XorPlus# commit
```

set poe power mode

The **set poe power mode** command configures PoE power mode to aggressive or redundant.

Command Syntax

set poe power mode <aggressive | redundant>

Parameter

Parameter	Description
mode <aggressive | redundant>	For details about the maximum power values supported by each PoE supported platform for the two PoE power modes, see Table 1.

Usage Guidelines

The maximum power value on S3410C-16TF-P does not distinguish between high and low voltages, and the POE supports a maximum power of 800 watts.

The maximum power value on S3410C-16TMS-P does not distinguish between high and low voltages, and the POE supports a maximum power of 800 watts.

The maximum power value on S3410L-24TF-P does not distinguish between high and low voltages, and the PoE power mode is only redundant with the maximum power value 800 Watts.

The maximum power value on S3410-24TS-P does not distinguish between high and low voltages, the maximum power value is 740 Watts in aggressive mode and 370 Watts in redundant mode**.**

The maximum power value on S5810-48TS-P, S5860-24XB-U and S3410C-8TMS-P does not distinguish between high and low voltages, the maximum power value is 1500 Watts in aggressive mode and 750 Watts in redundant mode**.**

The maximum power value on S5860-24MG-U does not distinguish between high and low voltages, the maximum power value is 648 Watts in aggressive mode and 324 Watts in redundant mode.

The maximum power value on S5860-48XMG-U does not distinguish between high and low voltages, the maximum power value is 765 Watts in aggressive mode and 382.5 Watts in redundant mode.

Table 1. The maximum power values supported by each PoE supported platform

Power Mode	High Voltage（Voltage>120V）		Low Voltage（Voltage<120V）	
	Aggressive (Watts)	Redundant (Watts)	Aggressive (Watts)	Redundant (Watts)
N3248PXE-ON	2496	1056	1261	406
N3248P-ON	1758	813	1568	713
N3208PX-ON	493	193	493	193
N3224PX-ON	2700	1260	1465	610
N3224P-ON	1771	826	1581	726
AS4610_54P	1500	750	800	400
AS4610_30P	1500	750	800	400
AS4630-54PE	1800	900	1000	500
AS4630-54NPE	1800	900	1000	500
N2248PX-ON	2714	1274	1479	624
N2224PX-ON	1757	812	1567	712
N3224P-ON	1771	826	1581	726
AS4625-54P	2025	945	1665	765

Example

- Configure power mode to aggressive.

```
admin@XorPlus# set poe power mode aggressive
```

```
admin@XorPlus# commit
```

set poe interface lldp-negotiation

This command is not available for S5810-48TS-P, S3410L-24TF-P, S5860-24XB-U, 3410C-16TMS-P, S3410C-8TMS-P and 3410C-16TF-P.

The **set poe interface lldp-negotiation** command is used to enable or disable PoE over LLDP power negotiation function on all ports or on a specific port.

Command Syntax

set poe interface <**all** | *interface-name*> **lldp-negotiation** <**true** | **false**>

Parameter

Parameter	Description
interface {**all** | *interface-name*}	Specifies an interface name. The value could be **all** or a specific interface name, **all** indicates a global configuration that enables or disables the PoE over LLDP power negotiation function on all ports.
lldp-negotiation {**true** | **false**}	Enables or disables the PoE over LLDP power negotiation function. The value is **true** or **false**. • **true**: enables the PoE over LLDP power negotiation function. • **false**: disables the PoE over LLDP power negotiation function. The default value is **true**.

Usage Guidelines

PoE over LLDP power negotiation function allows the switch to assign the power priority and power value provided by the powered device by using Link Layer Discovery Protocol (LLDP) power negotiation rather than the power priority and power value configured on the switch interface.

By default, PoE over LLDP power negotiation function is globally enabled for all the interfaces. It can be configured globally and per-interface, and the per-interface configuration takes a precedence over the global configuration.

When an expansion module is connected to the IP phone, in order to provide the required power to the expansion module, user should perform the following two operations to re-negotiate the PoE power supply.

1). Enable the PoE over LLDP power negotiation function on the interface by using **set poe interface** <**all** | *interface-name*> **lldp-negotiation** <**true** | **false**> command.

2). Disable and re-enable PoE function of the interface by using **set poe interface {**<*port-id*> | **all} enable <true | false>** command.

NOTE:

- Enable LLDP function and PoE function before using PoE over LLDP power negotiation.
- Enable PoE over LLDP power negotiation function when there is an expansion module connected to the IP phone.

Example

- Disable the PoE over LLDP power negotiation function on interface Ge-1/1/1.

```
admin@Xorplus# set poe interface ge-1/1/1 lldp-negotiation false
admin@Xorplus# commit
```

- Enable the PoE over LLDP power negotiation function on interface Ge-1/1/1.

```
admin@Xorplus# set poe interface ge-1/1/1 lldp-negotiation true
admin@Xorplus# commit
```

set poe power voltage

> **NOTE:**
> This command is applied on AS4630-54NPE and AS4630-54PE.

The **set poe power voltage** command configures PoE power voltage on AS4630-54NPE and AS4630-54PE platforms.

The **delete poe power voltage** command deletes the configuration.

Command Syntax

set poe power voltage [**110v | 220v**]

Parameters

Parameter	Description
voltage [**110v** | **220v**]	Specifies the voltage value. The value could be **110v** or **220v**.The default value is **110v**.

Usage Guidelines

On AS4630-54NPE and AS4630-54PE, PICOS cannot read out the voltage. Users can use command **set poe power voltage** [**110v | 220v**] to set PoE power voltage. With different voltage, 110V-120V at low-line or 220V-240V at high-line, each PSDU will give 1000W or 1200W respectively. Accordingly, the switch will allocate different power to PoE with regarding to low-line or high-line. By accounting for the PoE guard band (10%), the PoE available powers are illustrated by below table.

With two PSUs powered on:

Voltage / Power Mode	Low-line (110V)	High-line (220V)
redundant	700W x 90% = 630W	900W x 90% = 810W
aggressive	1700W x 90% = 1530W	2100W x 90% = 1890W

With one PSU powered on:

Voltage / Power Mode	Low-line (110V)	High-line (220V)
redundant	700W x 90% = 630W	900W x 90% = 810W
aggressive	700W x 90% = 630W	900W x 90% = 810W

Example

- Configure PoE power voltage on AS4630-54NPE or AS4630-54PE.

```
admin@Xorplus# set poe power voltage 110v
admin@Xorplus# commit
```

When PoE power mode is *redundant*, the result of “run show poe power” shows as below:

```
Total power allocated  RealTime consumption   Power available  Power Mode      PSU1 Status           PSU2 Status
---------------------  --------------------   ---------------  ----------      -----------           -----------
0.00W                  0.00W                  630.00W          redundant       Powered on            Powered on
```

When PoE power mode is *aggressive*, the result of “run show poe power” shows as below:

```
root@PICOS# run show poe power
Total power allocated  RealTime consumption   Power available  Power Mode      PSU1 Status           PSU2 Status
---------------------  --------------------   ---------------  ----------      -----------           -----------
0.00W                  0.00W                  1530.00W         aggressive      Powered on            Powered on
```

set protocols poe traceoptions flag all disable

The **set protocols poe traceoptions flag all disable** command can be used to enable or disable PoE debugging for tracing all PoE operations.

The **delete protocols poe traceoptions flag all disable** command deletes the configuration.

Command Syntax

set protocols poe traceoptions flag all disable <**true | false**>

delete protocols poe traceoptions flag all disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable PoE debugging for tracing all PoE operations. The value could be **true** or **false**. • **true**: Disable PoE debugging for tracing all PoE operations. • **false**: Enable PoE debugging for tracing all PoE operations. By default, the PoE debugging for tracing all PoE operations is disabled.

Example

- Enable PoE debugging for tracing all PoE operations.

```
admin@PICOS# set protocols poe traceoptions flag all disable false
admin@PICOS# commit

```

run show poe interface

The **run show poe interface** command displays the PoE status of all the ports or on a specific ethernet port.

Command Sytax

run show poe interface {<*port-id*> | **all**}

Parameter

Parameter	Description
interface {<*port-id*> | **all**}	Specifies interface ID. The value could be ge-1/1/1 to ge-1/1/48, **all** indicates to display PoE status of all the ports.

Example

• This example is to show poe interface of ge-1/1/1:

```
admin@XorPlus# run show poe interface ge-1/1/1
Port       Status    Consume   Reserved   Pair  PD_Type  PD-Class   Detection_Type
------------------------------------------------------------------------------
ge-1/1/1   Searching   2.80W    16.20W     A    IEEE          2     IEEE 802.3af 4-Point
```

• This example is to show poe interface of all the ports:

```
admin@XorPlus# run show poe interface all
Port       Status    Consume  Reserved Pair  PD_Type   PD-Class   Detection_Type
------------------------------------------------------------------------------
ge-1/1/1   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/2   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/3   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/4   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/5   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/6   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/7   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/8   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/9   Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/10  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/11  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/12  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/13  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/14  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/15  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/16  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/17  Searching  0.00W  0.00W      A    None    4   IEEE 802.3af 4-Point
ge-1/1/18  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/19  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/20  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/21  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/22  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/23  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/24  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/25  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/26  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/27  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/28  Delivering 1.10W  16.2W      A    IEEE    2    IEEE 802.3af 4-Point
ge-1/1/29  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/30  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/31  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/32  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/33  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/34  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/35  Delivering 1.30W  16.2W      A    IEEE    2    IEEE 802.3af 4-Point
```

```
ge-1/1/36  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/37  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/38  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/39  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/40  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/41  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/42  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/43  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/44  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/45  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/46  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/47  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
ge-1/1/48  Searching  0.00W  0.00W      A    None    4    IEEE 802.3af 4-Point
```

Table 1 Description of the run show poe interface all command output of AS4610-30P, AS4610-54P

Item	Description
Port	Port ID.
Status	Indicates that PoE function status, the value could be **Disabled**, **Searching**, **Delivering**, **Test**, **Requesting** and **Fault**.
Consume	Indicates the power consumption of port.

Reserved	Indicates the power allocated.
	• When PoE over LLDP power negotiation is enabled, it shows the negotiated power.
	• When PoE over LLDP power negotiation is disabled,
	  • If mangement mode is dynamic, the allocated power is same to the consumption power on AS4610-30P, AS4610-54P, AS4630-54PE and AS4630-54NPE
	  • If mangement mode is static, the allocated power is the configured max-power on AS4610-30P, AS4610-54P, AS4630-54PE and AS4630-54NPE.

Pair	Indicates PoE pair mode. **A**: signal, deliver power with data transmit cable. **B**: spare, deliver power with spare cable.
PD_Type	Indicates powered device type, the value could be **None**, **IEEE**, **Pre-Standard** and **Extended**.
PD_Class	Indicates the PD class, the value could be **1**, **2**, **3**, **4**.
Detection_Type	Indicates PoE detection type, the value could be: **no detection** **Legacy Capacitive Detection only** **IEEE 802.3af 4-Point Detection only** **IEEE 802.3af 4-Point followed by Legacy** **IEEE 802.3af 2-Point Detection** **IEEE 802.3af 2-Point followed by Legacy**

run show poe power

The **run show poe power** command displays the PoE power status.

Note:

On AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P and AS4630-54NPE,

- If Power Management mode is dynamic, total power allocated is about the same value as realtime consumption.
- But if Power Management mode is static, total power allocated is usually larger than realtime consumption.

On other PoE supported switches, regardless of whether Power Management mode is dynamic or static, the total power allocated is about the same value as realtime consumption.

Example

- Displays the PoE power status.

On AS4610-30P, AS4610-54P, AS4630-54PE, AS4625-54P, AS4630-54NPE, S5860-24XB-U, S5810-48TS-P, S5860-24MG-U, S5860-48XMG-U and S3410C-8TMS-P:

```
admin@XorPlus# run show poe power
Total power allocated           RealTime consumption     Power available   Power Mode    PSU1 Status    PSU2 Status
-------------------------------------------------------------------------------------------------------------------
2.20W                           2.20W                     675.00W         redundant       Powered on          Prese
```

On other PoE supported switches:

```
root@Xorplus# run show poe power
Consumption Power  Calculated Power  Available Power   PSU1 Status           PSU2 Status
-------------------------------------------------------------------------------------------------------------
0W                  0W               950W            Not present           Powered on
```

Table 1 Description of the run show poe power command output

Item	Description
Total power allocated	Total allocated max power for all ports.
RealTime consumption	The actual consumption power of all ports.
Power available	The max limit power value of PSE.
Consumption Power	The actual power consumed by all ports.
Calculated Power	The sum of all ports power, allocated as defined by IEEE standard 802.3af-2003, or actually consumed.
Available Power	The max limit power value of PSE.
Power Mode	Redundant or aggressive based on set.
PSU1 Status	Status of PSU1.
PSU2 Status	Status of PSU2.

VRRP Commands

- set protocols vrrp interface vrid
- set protocols vrrp interface vrid disable
- set protocols vrrp interface vrid version
- set protocols vrrp interface vrid ip
- set protocols vrrp interface vrid priority
- set protocols vrrp interface vrid interval
- set protocols vrrp interface vrid preempt enable
- set protocols vrrp interface vrid load-balance disable
- set protocols vrrp interface vrid load-balance virtual-mac time-interval
- set protocols vrrp interface vrid accept disable
- set protocols vrrp interface vrid authentication type
- set protocols vrrp interface vrid simple-key
- set protocols vrrp interface vrid md5-key
- run show vrrp
- set protocols vrrp interface vrid ipv6-nd adv-interval-option
- set protocols vrrp interface vrid ipv6-nd home-agent-config-flag
- set protocols vrrp interface vrid ipv6-nd home-agent-lifetime
- set protocols vrrp interface vrid ipv6-nd home-agent-preference
- set protocols vrrp interface vrid ipv6-nd managed-config-flag
- set protocols vrrp interface vrid ipv6-nd mtu
- set protocols vrrp interface vrid ipv6-nd other-config-flag
- set protocols vrrp interface vrid ipv6-nd prefix off-link
- set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime
- set protocols vrrp interface vrid ipv6-nd prefix router-address
- set protocols vrrp interface vrid ipv6-nd ra-fast-retrans
- set protocols vrrp interface vrid ipv6-nd ra-interval
- set protocols vrrp interface vrid ipv6-nd ra-lifetime
- set protocols vrrp interface vrid ipv6-nd reachable-time
- set protocols vrrp interface vrid ipv6-nd router-preference
- set protocols vrrp interface vrid ipv6-nd suppress-ra

set protocols vrrp interface vrid

The **set protocols vrrp interface vrid** command creates a VRRP group.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Usage Guidelines

When configuring VRID, pay attention to the following points:

- A VRID identifies the devices of the same VRRP group. Two devices in a VRRP group must be configured with the same VRID.
- It is recommended that VRRP groups on different L3 interfaces of a device should be configured with different VRIDs.
- One chassis switch supports a maximum of 128 VRRP groups. Please set the number of VRRP group based on device performance.

Example

- Create a VRRP group on vlan100 with VRID 2.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2
admin@Xorplus# commit
```

set protocols vrrp interface vrid disable

The **set protocols vrrp interface vrid disable** command is used to enable or disable the VRRP function.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **disable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
disable <**true	false**>	Enables or disables the VRRP function. The value is **true** or **false**. • **true**: disables the VRRP function. • **false**: enables the VRRP function. By default, VRRP function is enabled.

Example

- Disable the VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 disable true
admin@Xorplus# commit
```

- Enable the VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 disable false
admin@Xorplus# commit
```

set protocols vrrp interface vrid version

The **set protocols vrrp interface vrid version** command assigns the VRRP version on the VRRP-enabled device.

NOTE:

This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **version** <**2** | **3**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
version <**2** | **3**>	Specifies the VRRP version. The value could be **2** or **3**, indicating VRRPv2 or VRRPv3. By default, the system uses VRRPv2.

Usage Guidelines

VRRPv3 supports IPv4 and IPv6 address families while VRRPv2 only supports IPv4 addresses. That is,

- A VRRPv2 group can send and receive only VRRPv2 Advertisement packets. The VRRPv2 group discards the received VRRPv3 Advertisement packets.
- A VRRPv3 group can send and receive both VRRPv2 and VRRPv3 Advertisement packets.

NOTE:

- As VRRPv2 and VRRPv3 interoperation is not supported, VRRP version must be the same on both devices of a VRRP group. If the VRRP versions on the switches in the VRRP group are different, which may result in abnormal VRRP operation.
- When upgrading, we recommend that PICOS versions of the VRRP group devices be upgraded to PICOS 2.11.10 or later versions at the same time, as PICOS supports VRRPv3 from PICOS 2.11.10.

Example

- Assign the VRRP version.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 version 3
admin@Xorplus# commit
```

set protocols vrrp interface vrid ip

The **set protocols vrrp interface vrid ip** command assigns a virtual IP address to the VRRP group.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ip** <*ip-address*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
ip <*ip-address*>	Specifies the virtual IPvX address of a VRRP group. The value could be an IPv4 address or an IPv6 address. Type the IPvX address without subnet mask as the mask value is the same as the Layer 3 interface.

Usage Guidelines

If users on a network have the same reliability requirements, configure multiple virtual IPvX addresses for a VRRP group. By doing this, one virtual IP address can serve one separate user group.

One VRRP group supports a maximum of 254 virtual IPv4 addresses, and 64 virtual IPv6 addresses.

Follow the rules below when configuring the virtual IPv4 / IPv6 address:

- For IPv4, the virtual IPv4 of the VRRP group and the IPv4 address of the interface should be configured in the same network segment to ensure that the VRRP group can work normally.
- For IPv6, the global virtual IPv6 address of the VRRPv3 group and the global IPv6 address of the interface should be configured in the same network segment to ensure that the VRRPv3 group can work normally.
- The IP address of the virtual router can be either an unassigned IP address in the network segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group. A router whose interface IP address is the same as the virtual IP address is called an "IP address owner".
- The virtual IPv4 address of the VRRP group cannot be all zeros, broadcast address (255.255.255.255), network address or network broadcast address of the segment where the virtual IP address resides, loopback address, non-A / B / C address or any other illegal IP Address (e.g., 0.0.0.1).
- In the same VRRP group, IPv4 and IPv6 cannot be mixed. That is, the configured virtual IP addresses in the same VRRP group could either be virtual IPv4 addresses or virtual IPv6 addresses.
- For IPv6, configure at least one link-local IPv6 address in a VRRPv3 group which will be used as gateway address for the hosts, the format is FE80::/10.
- Virtual IP address list on both devices of VRRP group must be the same.
- Configure one or more global virtual IPv6 addresses, for the purpose of configuring global addresses via stateless address autoconfiguration of the downstream host (refer to RFC2462 IPv6 Stateless Address Autoconfiguration).

The gateway address of the downstream host should be configured as the virtual IPvX address of the VRRP virtual router device. For IPv6, the gateway address should be the virtual link-local address.

Example

- Assigns a virtual IP address to the VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ip 192.168.1.5
admin@Xorplus# commit
```

set protocols vrrp interface vrid priority

The **set protocols vrrp interface vrid priority** command sets the priority of the device in a VRRP group.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **priority** <*priority-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
priority <*priority-value*>	Specifies the priority of the device in a VRRP group. The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority. The default value is 100.

Usage Guidelines

VRRP determines the device role in the VRRP group based on device priority and L3 interface by exchanging VRRP advertisement packets. The device with a higher priority is more likely to become the master. If two devices have the same priority, the device with a larger interface IP address becomes the master.

The IP address owner's running priority is always 255, and no user configuration is required; the IP address owner always works in preemptive mode, regardless of whether the preemption function is enabled. If the VRRP device is the IP address owner, it will switch to the master state immediately after receiving the interface Up message.

For the backup device, if it has a higher priority than the master, the working mode of the backup (preemptive or non-preemptive) determines whether the master is re-selected.

- Preemptive mode: If the priority of the backup router is higher than the priority of the current master router, the backup router automatically becomes the master router.
- Non-preemptive mode: As long as the master router is working properly, the backup router with a higher priority cannot become the master router.

Example

- Set the priority of the switch in VRRP group 2 to 150 on the VLAN interface.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 priority 150
admin@Xorplus# commit
```

set protocols vrrp interface vrid interval

The **set protocols vrrp interface vrid interval** command sets the interval at which the VRRP device sends VRRP advertisement packets.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **interval** <*interval-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
interval <*interval-value*>	Specifies the interval at which the VRRP device sends VRRP advertisement packets. The value is an integer, in seconds. For VRRPv2, the value ranges from 1 to 255. For VRRPv3, the value ranges from 1 to 40. The default value is 4 seconds for both VRRPv2 and VRRPv3.

Usage Guidelines

If a larger interval is used, a backup device in the same VRRP group will not be able to detect the fault on the master in a timely fashion and can potentially cause packet loss. If a smaller interval is used, system resources are occupied. It is therefore recommended to set the interval based on actual network performance.

> **NOTE:**
> The configurations of the interval of sending VRRP advertisement packets on both devices of VRRP group must be the same.

Example

- Set the interval of sending VRRP advertisement to 5 seconds.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 interval 5
admin@Xorplus# commit
```

set protocols vrrp interface vrid preempt enable

The **set protocols vrrp interface vrid preempt enable** command configures the preemptive mode of the device in a VRRP group.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **preempt enable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
preempt enable <true | false>	Enables or disables the preemptive mode of the device. The value could be **true** or **false**. • **true**: enables the preemptive mode. Device in preemptive mode can preempt other nodes to be master if it has a higher priority. • **false**: disables the preemptive mode. Device in non-preemptive mode cannot preempt other nodes to be master even if it has the highest priority. By default, preemptive mode is enabled.

Usage Guidelines

To enable the device with higher priority in a VRRP group to be the master, set the preemptive mode on the device.

For the backup device, if it has a higher priority than the master, the working mode of the backup (preemptive or non-preemptive) determines whether the master is re-selected.

- Preemptive mode: If the priority of the backup router is higher than the priority of the current master router, the backup router automatically becomes the master router.
- Non-preemptive mode: As long as the master router is working properly, the backup router with a higher priority cannot become the master router.

By default, the preemptive mode is enabled, therefore, the device with a high priority is the master of the VRRP group.

> **NOTE:**
> The IP address owner always works in preemptive mode, regardless of whether the preemption function is enabled or not.

Example

- Enable the preemptive mode of the device in a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 preempt enable true
admin@Xorplus# commit
```

set protocols vrrp interface vrid load-balance disable

The **set protocols vrrp interface vrid load-balance disable** command is used to enable or disable the Active-Active VRRP function.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **load-balance disable** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
disable <**true	false**>	Enables or disables the Active-Active VRRP function. The value is **true** or **false**. • **true**: disables the Active-Active VRRP function. • **false**: enables the Active-Active VRRP function. By default, Active-Active VRRP function is disabled.

Usage Guidelines

In the Standard VRRP protocol mode, only the Virtual Master Router can forward packets whereas the Virtual Backup Routers cannot forward packets. By adding a new working mechanism based on the VRRP standard protocol mode, Active-Active VRRP mode provides load balancing between the master and backup switches in the VRRP group, both of which are active, thus avoiding the situation where the backup switches are always idle in the Standard VRRP protocol mode. This greatly improves efficiency of network resources.

NOTE:

- To make the Active-Active VRRP function take effect, enable VRRP function by using set protocols vrrp interface vrid disable command.
- The Active-Active VRRP mode must be enabled or disabled on both devices of VRRP group.

Example

- Disable the Active-Active VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 load-balance disable true
admin@Xorplus# commit
```

- Enable the Active-Active VRRP function.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 load-balance disable false
admin@Xorplus# commit
```

set protocols vrrp interface vrid load-balance virtual-mac time-interval

The **set protocols vrrp interface vrid load-balance virtual-mac time-interval** command sets the interval at which the VRRP device sends virtual MAC update packets.

> **NOTE:**
>
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **load-balance virtual-mac time-interval** <*interval-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
time-interval <*interval-value*>	Specifies the interval at which the VRRP device sends virtual MAC update packets. The value is an integer, in seconds, the value ranges from 60 to14400. The default value 120s.

Usage Guidelines

To notify the downstream device of the virtual MAC, the master and backup devices send periodic virtual MAC update messages. The virtual MAC address in Active-Active VRRP mode is used in the Ethernet header of virtual MAC update packet as the source MAC address. The connected network devices of the VRRP group refresh their MAC entries in time in order to forward packets.

Example

- Set the interval of sending virtual MAC update packets to 80 seconds.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 load-balance virtual-mac time-interval 80
admin@Xorplus# commit
```

set protocols vrrp interface vrid accept disable

The **set protocols vrrp interface vrid accept disable** command is used to enable or disable the Accept Mode of the device in a VRRP group.

NOTE:

As Accept Mode is only supported in VRRPv3, this command applies to only VRRPv3 configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **accept disable** <true | false>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
accept disable <true | false>	Enables or disables Accept Mode. The value could be **true** or **false**. • **true**: disables Accept Mode. • **false**: enables Accept Mode. By default, Accept Mode is disabled.

Usage Guidelines

VRRPv3 supports Accept Mode which controls whether a virtual router in Master state will accept packets addressed to the virtual IPvX address of a VRRP group if it is not the IP address owner (the IP address owner is the router that has the interface whose actual IP address is used as the virtual router's IP address).

By default, the Accept Mode is disabled, if the master is not the IP address owner, it only accepts the ARP requests/ARP replies or NS/NA messages addressed to the virtual IP, any other messages whose destination IP is the virtual IP are not accepted. But when accept mode is enabled, it can accept all packets whose destination IP is a virtual IP.

Deployments that rely on, for example, pinging the address owner's IPvX address may choose to configure Accept Mode to True.

NOTE:

- Accept Mode is only supported in VRRPv3 while VRRPv2 does NOT support. In VRRPv2, the master switch always accepts packets addressed to the virtual IPvX address.
- When Accept Mode is disabled, PICOS can still accept and process IPv6 Neighbor Solicitations / Neighbor Advertisements packets and ARP Request / ARP Reply packets.
- If the master is the IP address owner, it accepts all the packets addressed to the IPvX address(es) associated with the virtual router even though Accept Mode is disabled.

Example

- Enable the accept mode of the device in VRRP group 2.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 accept disable false
admin@Xorplus# commit
```

set protocols vrrp interface vrid authentication type

The **set protocols vrrp interface vrid authentication type** command configures an authentication mode for a VRRP group.

> **NOTE:**
> VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication type** <**none** | **md5** | **simple**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
authentication type <none | md5 | simple>	Specifies the authentication mode. The value could be **none**, **md5** or **simple**. • **none**: Indicates no authentication. • **md5**: Indicates MD5 authentication. • **simple**: Indicates simple authentication. By default, there's no authentication.

Usage Guidelines

NOTE:

- Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.
- If the VRRP authentication fails, the system prints the warning level log.

Example

- Enable MD5 authentication mode for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 authentication type md5
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 md5-key picos123
admin@Xorplus# commit
```

set protocols vrrp interface vrid simple-key

The **set protocols vrrp interface vrid authentication simple-key** command configures the authentication key in simple authentication mode for a VRRP group.

> **NOTE:**
> VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **authentication simple-key** <*simple-key*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
authentication simple-key <*simple-key*>	Specifies the authentication key in simple authentication mode. The value is a string of 1 to 8 case-sensitive characters without spaces.

Usage Guidelines

> **NOTE:**
> Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.

Example

- Configure the authentication key in simple authentication mode for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 authentication simple-key picos123
admin@Xorplus# commit
```

set protocols vrrp interface vrid md5-key

The **set protocols vrrp interface vrid md5-key** command configures the authentication key in MD5 authentication mode for a VRRP group.

> **NOTE:**
> VRRP authentication is only supported by VRRPv2, which is not supported by VRRPv3.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **md5-key** <*md5-key*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
md5-key <*md5-key*>	Specifies the authentication key in MD5 authentication mode. The value is a string of 1 to 16 case-sensitive characters without spaces.

Usage Guidelines

> **NOTE:**
> Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.

Example

- Configure the authentication key in MD5 authentication mode for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 md5-key picos123
admin@Xorplus# commit
```

run show vrrp

The **run show vrrp** command displays the configuration information of VRRP group.

> **NOTE:**
> This command applies to both VRRPv2 and VRRPv3 configuration.

Command Syntax

run show vrrp *<interface-name>*

Parameter

Parameter	Description
<interface-name>	Optional. Specifies the Layer 3 interface name of VRRP device. The value is a string.

Example

- Run **run show vrrp** command to view the configuration information of VRRP group.

```
admin@XorPlus# run show vrrp vlan100
Interface: vlan100
VRID: 1
Version:                    3
Accept:  disable
Load-balance: enable
State: Master
Master IP: 192.168.1.1
Virtual MAC: 00:00:5e:00:01:01
Preempt: enable
Adver Interval: 4
Priority: 250
Virtual IP: 192.168.1.5
Auth-type:                  simple
Auth-key:                   123456
```

set protocols vrrp interface vrid ipv6-nd adv-interval-option

The **set protocols vrrp interface vrid ipv6-nd adv-interval-option** command includes an Advertisement Interval option which indicates to hosts the maximum time, in milliseconds, between successive unsolicited Router Advertisements for a VRRP group. Default: not set.

The **delete protocols vrrp interface vrid ipv6-nd adv-interval-option** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd adv-interval-option**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Example

- Configure to include an Advertisement Interval option between successive unsolicited Router Advertisements for a VRRP group.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd adv-interval-option
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd home-agent-config-flag

The **set protocols vrrp interface vrid ipv6-nd home-agent-config-flag** command sets flag in IPv6 router advertisements which indicates to hosts that the router acts as a Home Agent and includes a Home Agent Option. Default: not set.

The **delete protocols vrrp interface vrid ipv6-nd home-agent-config-flag** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd home-agent-config-flag**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Example

- Configure to set flag in IPv6 router advertisements which indicates to hosts that the router acts as a Home Agent and includes a Home Agent Option.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd home-agent-config-flag
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd home-agent-lifetime

The **set protocols vrrp interface vrid ipv6-nd home-agent-lifetime** command sets the value to be placed in Home Agent Option, when Home Agent config flag is set, which indicates to hosts Home Agent Lifetime.

The **delete protocols vrrp interface vrid ipv6-nd home-agent-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd home-agent-lifetime** <*home-agent-lifetime*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
home-agent-lifetime <*home-agent-lifetime*>	Specifies the lifetime of the home agent. The value is an integer, in seconds, that ranges from 0 to 65520. The default value of 0 means to place the current Router Lifetime value.

Example

- Configure the lifetime of the home agent to 120 seconds.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd home-agent-lifetime 120
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd home-agent-preference

The **set protocols vrrp interface vrid ipv6-nd home-agent-preference** command sets the value to be placed in Home Agent Option, when Home Agent config flag is set, which indicates to hosts Home Agent preference.

The **delete protocols vrrp interface vrid ipv6-nd home-agent-preference** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd home-agent-preference** <*home-agent-preference*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
home-agent-preference <*home-agent-preference*>	Specifies the preference of the home agent. The value is an integer, that ranges from 0 to 65535. The default value of 0 stands for the lowest preference possible. Default: 0.

Example

- Configure the preference of the home agent to 100.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd home-agent-preference 100
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd managed-config-flag

The **set protocols vrrp interface vrid ipv6-nd managed-config-flag** command controls flag setting in RAs the router transmits on the current interface. Enable the flag to indicate that hosts can obtain IP address through DHCPv6. The flag is disabled by default.

The **delete protocols vrrp interface vrid ipv6-nd managed-config-flag** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd managed-config-flag**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Example

- Configure the flag in IPv6 router advertisements which indicates to hosts that they should use managed (stateful) protocol for addresses autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd managed-config-flag
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd mtu

The **set protocols vrrp interface vrid ipv6-nd mtu** command configures the MTU size to be sent in the RA messages.

The **delete protocols vrrp interface vrid ipv6-nd mtu** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd mtu** <*mtu-value*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
mtu <*mtu-value*>	Specifies the MTU size. Range: 1-65535 bytes.

Example

- Configure the MTU size to 1500 bytes.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd mtu 1500
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd other-config-flag

The **set protocols vrrp interface vrid ipv6-nd other-config-flag** command sets the flag in IPv6 router advertisements which indicates to hosts that they should use DHCPv6 protocol to obtain autoconfiguration information other than addresses. Default: not set.

The **delete protocols vrrp interface vrid ipv6-nd other-config-flag** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd other-config-flag**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.

Example

- Configure the flag in IPv6 router advertisements which indicates to hosts that they should use DHCPv6 protocol to obtain autoconfiguration information other than addresses.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd other-config-flag
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix off-link

The **set protocols vrrp interface vrid ipv6-nd prefix off-link** command configures that advertisement makes no statement about on-link or off-link properties of the prefix. Default: not set, i.e. this prefix can be used for on-link determination.

The **delete protocols vrrp interface vrid ipv6-nd prefix off-link** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **off-link [no-autoconfig]**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.
no-autoconfig	Optional. Specifies do not use prefix for autoconfiguration. Default: not set, i.e. prefix can be used for autoconfiguration.

Example

- Configure that advertisement makes no statement about on-link or off-link properties of the prefix.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 off-link
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime

The **set protocols vrrp interface vrid ipv6-nd prefix valid-lifetime** command configures the length of time in seconds during what the prefix is valid for the purpose of onlink determination.

The **delete protocols vrrp interface vrid ipv6-nd prefix valid-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **valid-lifetime {**<*LIFETIME-VALUE*>**|infinite}**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.
valid-lifetime {<*LIFETIME-VALUE*>**|infinite}**	Specifies the length of time in seconds during what the prefix is valid for the purpose of onlink determination. Value **infinite** represents infinity (i.e. a value of all one bits (0xffffffff)). Range: (0-4294967295) Default: 2592000

Example

- Configure the length of time in seconds during what the prefix is valid for the purpose of onlink determination.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 valid-lifetime 2592000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime

The **set protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime** command configures the length of time in seconds during what addresses generated from the prefix remain preferred.

The **delete protocols vrrp interface vrid ipv6-nd prefix preferred-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **preferred-lifetime {**<*LIFETIME-VALUE*>**|infinite}**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.
preferred-lifetime {<*LIFETIME-VALUE*>**|infinite}**	Specifies the length of time in seconds during what addresses generated from the prefix remain preferred. Value infinite represents infinity. Range: (0-4294967295) Default: 604800.

Example

- Configure the length of time in seconds during what addresses generated from the prefix remain preferred. Value infinite represents infinity.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 preferred-lifetime 604800
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd prefix router-address

The **set protocols vrrp interface vrid ipv6-nd prefix router-address** command configures the router-address, indicating to hosts on the local link that the specified prefix contains a complete IP address by setting R flag. Default: not set, i.e. hosts do not assume a complete IP address is placed.

The **delete protocols vrrp interface vrid ipv6-nd prefix router-address** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd prefix** <*IPv6Net*> **router-address**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
prefix <*IPv6Net*>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M.

Example

- Configure the router-address, indicating to hosts on the local link that the specified prefix contains a complete IP address by setting R flag.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd prefix fa00::0/64 router-address
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd ra-fast-retrans

The **set protocols vrrp interface vrid ipv6-nd ra-fast-retrans** command can be used to enable or disable IPv6 nd ra-fast-retrans.

The **delete protocols vrrp interface vrid ipv6-nd ra-fast-retrans** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd ra-fast-retrans** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
ra-fast-retrans <**true	false**>	Enable or disable IPv6 nd ra-fast-retrans. • **true**: Enable IPv6 nd ra-fast-retrans. • **false**: Disable IPv6 nd ra-fast-retrans. By default, IPv6 nd ra-fast-retrans is enabled.

Usage Guidelines

RFC4861 states that consecutive RA packets should be sent no more frequently than three seconds apart. FRR by default allows faster transmissions of RA packets in order to speed convergence and neighbor establishment, particularly for unnumbered peering. By turning off ipv6 nd ra-fast-retrans, the implementation is compliant with the RFC at the cost of slower convergence and neighbor establishment.

Example

- Disable IPv6 nd ra-fast-retrans.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd ra-fast-retrans false
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd ra-interval

The **set protocols vrrp interface vrid ipv6-nd ra-interval** command configures the maximum time allowed between sending unsolicited multicast router advertisements from the interface.

The **delete protocols vrrp interface vrid ipv6-nd ra-interval** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd ra-interval** {**msec** <*interval1*> **| sec** <*interval2*>}

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
msec <*interval1*>	Specifies the maximum time between sending unsolicited multicast router advertisements from the interface in milliseconds. The value is an integer that ranges from 70 to 1800000. Default: 600000.
sec <*interval2*>	Specifies the maximum time between sending unsolicited multicast router advertisements from the interface in seconds. The value is an integer that ranges from 1 to 1800. Default: 600.

Example

- Configure the maximum time allowed between sending unsolicited multicast router advertisements from the interface.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd ra-interval msec 600000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd ra-lifetime

The **set protocols vrrp interface vrid ipv6-nd ra-lifetime** command configures the lifetime, in seconds, for the routing switch to be used as a default router by hosts on the current interface.

The **delete protocols vrrp interface vrid ipv6-nd ra-lifetime** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd ra-lifetime** <*time*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
ra-lifetime <*time*>	Specifies lifetime in seconds of a default router. A setting of 0 for default router lifetime in an RA indicates that the routing switch is not a default router on the interface. Range: 0-9000 seconds. Default: 1800 seconds.

Example

- Configure the lifetime for the routing switch to be used as a default router by hosts on the current interface.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd ra-lifetime 2000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd reachable-time

The **set protocols vrrp interface vrid ipv6-nd reachable-time** command configures the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

The **delete protocols vrrp interface vrid ipv6-nd reachable-time** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd reachable-time** <*time*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
reachable-time <*time*>	Specifies the reachable time in milliseconds. Range: 1-3600000. Default: 0 (no limit).

Example

- Configure the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd reachable-time 2000
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd router-preference

The **set protocols vrrp interface vrid ipv6-nd router-preference** command specifies the value that is set in the Default Router Preference (DRP) field of Router Advertisements (RAs) that the switch sends from an interface. An interface with a DRP value of high will be preferred by other devices on the network over interfaces with an RA value of medium or low.

The **delete protocols vrrp interface vrid ipv6-nd router-preference** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd router-preference** <**high | medium | low**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
router-preference <**high	medium	low**>	Specifies the value that is set in the Default Router Preference (DRP) field. • **high**: Sets DRP to high. • **medium**: Sets DRP to medium. Default. • **low**: Sets DRP to low.

Example

- Configure the value that is set in the Default Router Preference (DRP) field of Router Advertisements (RAs).

```
admin@Xorplus# set protocols vrrp interface vlan100 vrid 2 ipv6-nd router-preference high
admin@Xorplus# commit
```

set protocols vrrp interface vrid ipv6-nd suppress-ra

The **set protocols vrrp interface vrid ipv6-nd suppress-ra** command can be used to enable or disable sending Router Advertisement (RA) on specified VRRP interface. By default, PICOS do not send RA packets on VRRP interfaces.

The **delete protocols vrrp interface vrid ipv6-nd suppress-ra** command restores the default configuration.

Command Syntax

set protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd suppress-ra** <**true | false**>

delete protocols vrrp interface <*interface-name*> **vrid** <*virtual-router-id*> **ipv6-nd suppress-ra**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the Layer 3 interface name of VRRP device. The value could be the VLAN interface name, the routed interface or the sub-interface name. The value is a string.
vrid <*virtual-router-id*>	Specifies the VRID of a VRRP group. The value is an integer that ranges from 1 to 254.
<**true	false**>	Enable or disable sending RA packets on specified interface. The value could be **true** or **false**. • **true**: Disables sending RA packets. • **false**: Enables sending RA packets. By default, PICOS do not send RA packets on VRRP interfaces.

Example

- Enable sending RA packets on VLAN interface vlan10.

```
admin@Xorplus# set protocols vrrp interface vlan10 vrid 32 ipv6-nd suppress-ra false
admin@Xorplus# commit
```

Spanning Tree Protocol Commands

- run show spanning-tree
- run show spanning-tree mstp
- run show spanning-tree pvst
- run show spanning-tree rstp
- run show spanning-tree statistics
- run show spanning-tree stp
- set protocols spanning-tree enable
- set protocols spanning-tree force-version
- set protocols spanning-tree interface enable
- set protocols spanning-tree mstp bridge-priority
- set protocols spanning-tree mstp configuration-name
- set protocols spanning-tree mstp forward-delay
- set protocols spanning-tree mstp hello-time
- set protocols spanning-tree mstp interface bpdu-filter
- set protocols spanning-tree mstp interface bpdu-guard
- set protocols spanning-tree mstp interface edge
- set protocols spanning-tree mstp interface external-path-cost
- set protocols spanning-tree mstp interface internal-path-cost
- set protocols spanning-tree mstp interface manual-forwarding
- set protocols spanning-tree mstp interface mode
- set protocols spanning-tree mstp interface port-priority
- set protocols spanning-tree mstp interface root-guard
- set protocols spanning-tree mstp interface tcn-guard
- set protocols spanning-tree mstp max-age
- set protocols spanning-tree mstp max-hops
- set protocols spanning-tree mstp msti bridge-priority
- set protocols spanning-tree mstp msti interface cost
- set protocols spanning-tree mstp msti interface port-priority
- set protocols spanning-tree mstp msti vlan
- set protocols spanning-tree mstp revision-level
- set protocols spanning-tree pvst interface bpdu-guard
- set protocols spanning-tree pvst interface manual-forwarding
- set protocols spanning-tree pvst interface mode
- set protocols spanning-tree pvst interface root-guard
- set protocols spanning-tree pvst vlan bridge-priority
- set protocols spanning-tree pvst vlan enable
- set protocols spanning-tree pvst vlan forward-delay
- set protocols spanning-tree pvst vlan hello-time
- set protocols spanning-tree pvst vlan interface path-cost
- set protocols spanning-tree pvst vlan max-age
- set protocols spanning-tree rstp bridge-priority
- set protocols spanning-tree rstp forward-delay
- set protocols spanning-tree rstp hello-time
- set protocols spanning-tree rstp interface bpdu-filter
- set protocols spanning-tree rstp interface bpdu-guard
- set protocols spanning-tree rstp interface edge
- set protocols spanning-tree rstp interface mode
- set protocols spanning-tree rstp interface path-cost
- set protocols spanning-tree rstp interface port-priority
- set protocols spanning-tree rstp interface root-guard
- set protocols spanning-tree rstp interface tcn-guard
- set protocols spanning-tree rstp max-age
- set protocols spanning-tree stp bridge-priority
- set protocols spanning-tree stp forward-delay
- set protocols spanning-tree stp hello-time
- set protocols spanning-tree stp interface bpdu-filter
- set protocols spanning-tree stp interface bpdu-guard
- set protocols spanning-tree stp interface edge
- set protocols spanning-tree stp interface mode
- set protocols spanning-tree stp interface path-cost
- set protocols spanning-tree stp interface port-priority

- set protocols spanning-tree stp interface root-guard
- set protocols spanning-tree stp interface tcn-guard
- set protocols spanning-tree stp max-age

run show spanning-tree

The **run show spanning-tree** command displays the configuration information and status of spanning tree.

Command Syntax

run show spanning-tree

Parameter

None.

Example

- Run **run show spanning-tree** command to view the configuration information and status of spanning tree.

```
admin@PICOS# run show spanning-tree
--------------------------------------------------
Bridge Spanning Tree Parameters
  Enabled Protocol: MSTP
  Root ID: 32768.3c:2c:30:10:20:83
  External Root Path Cost: 0
  CIST Regional Root ID: 32768.3c:2c:30:10:20:83
  Root Port: te-1/1/1
  CIST Internal Root Path Cost: 800
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 19
  Bridge Configuration Name: Pica8
  Bridge Revision Level: 0
  Bridge Configuration Digest: ac36177f50283cd4b83821d8ab26de62
  Number of Topology Changes: 1
  Time Since Last Topology Change: 0 day 00:00:56
Local Parameters
  Bridge ID: 32768.8c:ea:1b:32:1f:58
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 20
```

run show spanning-tree mstp

The **run show spanning-tree mstp** command displays the configuration information and status of spanning tree protocol MSTP.

Command Syntax

run show spanning-tree mstp <**bridge** | **interface**> [**all** | **cist** | **msti** <*msti_num*>]

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**.
[**all** | **cist** | **msti** <*msti_num*>]	Optional. The value could be **all**, **cist** or **msti** <*msti_num*>. • **all**: Indicates to show the MSTP information of all the MSTIs. • **cist**: Indicates to show the MSTP information of CIST. • **msti** <*msti_num*>: Specifies the MST instance number. Indicates to show the MSTP information of a specific MSTI.

Example

- Run **run show spanning-tree mstp** command to view the configuration information and status of spanning tree protocol MSTP.

```
admin@PICOS# run show spanning-tree mstp bridge all
--------------------------------------------------
Bridge Spanning Tree Parameters
  Enabled Protocol: MSTP
  Root ID: 32768.3c:2c:30:10:20:83
  External Root Path Cost: 0
  CIST Regional Root ID: 32768.3c:2c:30:10:20:83
  Root Port: te-1/1/1
  CIST Internal Root Path Cost: 800
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 19
  Bridge Configuration Name: Pica8
  Bridge Revision Level: 0
  Bridge Configuration Digest: ac36177f50283cd4b83821d8ab26de62
  Msti 2 Member VLANs:
  Number of Topology Changes: 1
  Time Since Last Topology Change: 0 day 00:04:31
Local Parameters
  Bridge ID: 32768.8c:ea:1b:32:1f:58
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Remaining Hops: 20
--------------------------------------------------
STP Bridge Parameters for MSTI 2
  MSTI Regional Root: 32770.8c:ea:1b:32:1f:58
  Root Cost: 0
  Root Port:
  Hello Time: 2
  Max Age: 20
  Forward Delay: 15
  Remaining Hops: 20
  Time Since Last Topology Change: 0 day 00:05:15
Local Parameters
  Bridge ID: 32770.8c:ea:1b:32:1f:58
```

run show spanning-tree pvst

The **run show spanning-tree pvst** command displays the configuration information and status of spanning tree protocol Rapid PVST+.

Command Syntax

run show spanning-tree pvst <**bridge** | **interface**> [**all** | **vlan** <*vlan-id*>]

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**.
[**all** | **vlan** <*vlan-id*>]	The value could be **all**, **vlan** <*vlan-id*>. • **all**: Indicates to show the Rapid PVST+ information of all the VLANs. • **vlan** <*vlan-id*>: Specifies the VLAN ID. Indicates to show the Rapid PVST+ information of a specific VLAN. Optional when showing the spanning tree information based on **bridge**. Required when showing the spanning tree information based on **interface**.

Example

- Run **run show spanning-tree pvst** command to view the configuration information and status of spanning tree protocol Rapid PVST+.

```
admin@PICOS# run show spanning-tree pvst interface all

Rapid PVST+ Spanning Tree Interface Status for VLAN 1
Interface   Port ID    Designated  Designated Bridge        Path Cost  State       Role
                       Port ID     ID
----------  ---------  ----------  ----------------------  ---------  ----------  ---------------
te-1/1/1    128.1      128.1       32768.3c:2c:30:10:20:83  800        FORWARDING  ROOT



admin@PICOS# run show spanning-tree pvst bridge
-------------------------------------------------
Bridge Spanning Tree Parameters
  Enabled Protocol: PVST
  Root ID: 32768.3c:2c:30:10:20:83
  Root Path Cost: 800
  Designated Bridge ID: 32768.3c:2c:30:10:20:83
  Root Port: te-1/1/1
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
  Number of Topology Changes: 1
  Time Since Last Topology Change: 0 day 00:00:35
Local Parameters
  Bridge ID: 32769.8c:ea:1b:32:1f:58
  Hello Time: 2
  Maximum Age: 20
  Forward Delay: 15
```

run show spanning-tree rstp

The **run show spanning-tree rstp** command displays the configuration information and status of spanning tree protocol RSTP.

Command Syntax

run show spanning-tree rstp <**bridge** | **interface**>

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**.

Example

- Run **run show spanning-tree rstp** command to view the configuration information and status of spanning tree protocol RSTP.

```
admin@PICOS# run show spanning-tree rstp interface

RSTP Spanning Tree Interface Status
Interface   Port ID    Designated  Designated Bridge        Path Cost  State       Role
                       Port ID     ID
----------  ---------  ----------  ----------------------  ---------  ----------  ---------------
te-1/1/1    128.1      128.1       32768.3c:2c:30:10:20:83  800        FORWARDING  ROOT
```

run show spanning-tree statistics

The **run show spanning-tree statistics** command displays the statistics information of spanning tree.

Command Syntax

run show spanning-tree statistics [**interface** <*interface-name*>]

Parameter

Parameter	Description
<*interface-name*>	Optional. Specifies a interface name. It can be a physical interface or a LAG interface. Use this parameter to show the spanning tree statistics information of a specific interface.

Example

- Run **run show spanning-tree statistics** command to view the statistics information of spanning tree.

```
admin@PICOS# run show spanning-tree statistics
Interface   BPDU Rx Count  BPDU Tx Count
----------  -------------  -------------
te-1/1/1    173            50
```

run show spanning-tree stp

The **run show spanning-tree stp** command displays the configuration information and status of spanning tree protocol STP.

Command Syntax

run show spanning-tree stp <**bridge** | **interface**>

Parameter

Parameter	Description
<**bridge** | **interface**>	Indicates to show the spanning tree information based on **bridge** or **interface**.

Example

- Run **run show spanning-tree stp** command to view the configuration information and status of spanning tree protocol STP.

```
admin@PICOS# run show spanning-tree stp interface

STP Spanning Tree Interface Status
Interface   Port ID    Designated  Designated Bridge        Path Cost  State       Role
                       Port ID     ID
----------  ---------  ----------  ----------------------  ---------  ----------  ---------------
te-1/1/1    128.1      128.1       32768.3c:2c:30:10:20:83  800        DISCARDING  ROOT
```

set protocols spanning-tree enable

The **set protocols spanning-tree enable** command is used to enable or disable spanning tree protocols on a switching device.

Command Syntax

set protocols spanning-tree enable <**true** | **false**>

Parameter

Parameter	Description
enable <**true	false**>	Enables or disables spanning tree protocols. The value could be **true** or **false**. • **true**: enables spanning tree protocols. • **false**: disables spanning tree protocols. By default, spanning tree protocols is enabled.

Usage Guidelines

To enable a spanning tree protocol, use the **set protocols spanning-tree enable true** command first, then use the **set protocols spanning-tree force-version** <**0** | **2** | **3** | **4**> command to specify the protocol version.

Note: To enable Rapid-PVST+, you must also enable Rapid-PVST+ on the VLAN by using the **set protocols spanning-tree pvst vlan** <*vlan-id*> **enable true** command.

Example

- Disable spanning tree protocols.

```
admin@Xorplus# set protocols spanning-tree enable false
admin@Xorplus# commit
```

- Enable spanning tree protocols.

```
admin@Xorplus# set protocols spanning-tree enable true
admin@Xorplus# commit
```

set protocols spanning-tree force-version

The **set protocols spanning-tree force-version** command sets the version of the spanning tree protocol on a switching device.

Command Syntax

set protocols spanning-tree force-version <**0 | 2 | 3 | 4**>

Parameter

Parameter	Description
force-version <**0** | **2**| **3** | **4**>	Specifies the version of the spanning tree protocol. The value could be **0**, **2**, **3** or **4**. • **0**: Indicates the STP mode. • **2**: Indicates the RSTP mode. • **3**: Indicates the MSTP mode. • **4**: Indicates the Rapid-PVST+ mode. The default spanning tree protocol is MSTP.

Usage Guidelines

A switch has four operation modes: Rapid-PVST+, MSTP, RSTP, and STP. On the network running a spanning tree protocol, switches running different spanning tree protocols cannot communicate with each other. As a result, spanning trees cannot be properly calculated.

Example

- Set the version of the spanning tree protocol to Rapid-PVST+.

```
admin@Xorplus# set protocols spanning-tree force-version 4
admin@Xorplus# commit
```

set protocols spanning-tree interface enable

The **set protocols spanning-tree interface enable** command can be used to enable or disable spanning tree protocol on a specific interface.

The **delete protocols spanning-tree interface enable** command deletes the configuration.

Command Syntax

set protocols spanning-tree interface <*interface-name*> **enable** <**true | false**>

delete protocols spanning-tree interface <*interface-name*> **enable**

Parameters

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value is a physical port or an LAG port.
enable <**true	false**>	Enable or disable spanning tree protocol on a specific interface. The value could be **true** or **false**. • **true**: Enable spanning tree protocol. • **false**: Disable spanning tree protocol. By default, spanning tree protocol is enabled.

Example

- Disable spanning tree protocol on interface te-1/1/7.

```
admin@PICOS# set protocols spanning-tree interface te-1/1/7 enable false
admin@PICOS# commit
```

set protocols spanning-tree mstp bridge-priority

The **set protocols spanning-tree mstp bridge-priority** command sets the bridge priority of the switching device when MSTP is running.

Command Syntax

set protocols spanning-tree mstp bridge-priority <*bridge-priority*>

Parameter

Parameter	Description
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device when MSTP is running. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree mstp configuration-name

The **set protocols spanning-tree mstp configuration-name** command configures the MST region name of the switching device.

Command Syntax

set protocols spanning-tree mstp configuration-name <*configuration-name*>

Parameter

Parameter	Description
configuration-name <*configuration-name*>	Specifies the MST region name. The value is a string.

Usage Guidelines

MST region name is used to distinguish MST regions. Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

Example

- Configure the MSTP bridge configuration name.

```
admin@Xorplus# set protocols spanning-tree mstp configuration-name mstp1
admin@Xorplus# commit
```

set protocols spanning-tree mstp forward-delay

The **set protocols spanning-tree mstp forward-delay** command sets the value of the MSTP forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree mstp forward-delay <*forward-delay*>

Parameter

Parameter	Description
forward-delay <*forward-delay*>	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the MSTP forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree mstp forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree mstp hello-time

The **set protocols spanning-tree mstp hello-time** command sets the interval of the switching device to send BPDUs when MSTP is running.

Command Syntax

set protocols spanning-tree mstp hello-time <*hello-time*>

Parameter

Parameter	Description
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface bpdu-filter

The **set protocols spanning-tree mstp interface bpdu-filter** command configures a physical port or a LAG port as a BPDU-filter port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **bpdu-filter** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-filter <**true** | **false**>	Enables or disables BPDU-filter on a port. The value could be **true** or **false**. • **true**: enables BPDU-filter. • **false**: disables BPDU-filter. By default, BPDU-filter is disabled.

Usage Guidelines

When configuring a port as a BPDU-filter port, the port will not process BPDUs.

NOTE:

If the port is set to the BPDU filter port, the port does not participate in spanning tree calculation, so it is recommended to configuring BPDU-filter port only on edge ports.

Example

- Configure the port ge-1/1/1 as a BPDU-filter port.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 bpdu-filter true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface bpdu-guard

The **set protocols spanning-tree mstp interface bpdu-guard** command configures a physical port or a LAG port as a BPDU-guard port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree mstp interface** <*interface-name*> **bpdu-guard** true command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** command manually.

Example

- Configure the port ge-1/1/1 as a BPDU-guard port.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface edge

The **set protocols spanning-tree mstp interface edge** command configures a physical port or a LAG port as an edge port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **edge** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
edge <**true	false**>	Enables or disables edge on a port. The value could be **true** or **false**. • **true**: enables a physical or a LAG port as an edge port. • **false**: disables a physical or a LAG port as an edge port. The default value is false.

Usage Guidelines

The edge port does not participate in the spanning tree calculation. However, once the edge port receives a configuration BPDU, the switching device automatically sets the edge port to a non-edge port and performs spanning tree calculation again.

Example

- Configure the port ge-1/1/1 as an edge port port.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 edge true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface external-path-cost

The **set protocols spanning-tree mstp interface external-path-cost** command configures the path cost of the external link on a physical port or a LAG port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **external-path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
external-path-cost <*path-cost*>	Specifies the path cost value of the external link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

External path cost indicates the path cost from a CIST regional root to the root. External path cost saved on all switching devices in an MST region are same. If the CIST root is in an MST region, external path cost saved on all switching devices in the MST region are 0s.

Note: When the path cost value changes, the spanning tree will be recalculated.

Example

- Configure the path cost of the external link on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 external-path-cost 500
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface internal-path-cost

The **set protocols spanning-tree mstp interface internal-path-cost** command configures the path cost of the internal link on a physical port or a LAG port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **internal-path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
internal-path-cost <*path-cost*>	Specifies the path cost value of the internal link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Indicates the path cost from the local bridge to the regional root. The internal path cost saved on a regional edge port is greater than that saved on a non-regional edge port.

Example

- Configure the path cost of the internal link on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 internal-path-cost 1248
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface manual-forwarding

The **set protocols spanning-tree mstp interface manual-forwarding** command manually configures a physical port or a LAG port as a forwarding port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **manual-forwarding** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
manual-forwarding <**true**	**false**>	Manually configure a physical port or a LAG port as a forwarding port. The value could be **true** or **false**. • **true**: manually configures a physical port or a LAG port as a forwarding port. • **false**: disables manual forwarding on a port. By default, manual forwarding is disabled.

Usage Guidelines

After manually configuring a physical port or a LAG port as a forwarding port, the state of the port is always forwarding, unless the port is down. The port does not participate in spanning tree calculation and does not send and receive BPDUs.

Example

- Configure the port ge-1/1/1 as a forwarding port manually for MSTP mode.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 manual-forwarding true
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface mode

The **set protocols spanning-tree mstp interface mode** command configures the link type of a port. The setting for port duplex mode applies to this port on all MST instances.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point**	**shared**>	Specifies the link type of the port. The value could be **point-to-point** or **shared**. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface port-priority

The **set protocols spanning-tree mstp interface port-priority** command configures the priority of a port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Configure the port priority of ge-1/1/1 to 15.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 port-priority 15
admin@Xorplus# commit
```

set protocols spanning-tree mstp interface root-guard

The **set protocols spanning-tree mstp interface root-guard** command is used to enable or disable root guard function for MSTP.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name.
root-guard <**true**	**false**>	Enables or disables root guard function for MSTP. The value could be **true** or **false**. • **true**: enables root guard function for MSTP. • **false**: disables root guard function for MSTP. By default, root guard function for MSTP is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for MSTP on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 root-guard true
```

set protocols spanning-tree mstp interface tcn-guard

The **set protocols spanning-tree mstp interface tcn-guard** command configures TCN (Topology Change Notification) guard on a physical port or a LAG port for MSTP mode.

Command Syntax

set protocols spanning-tree mstp interface <*interface-name*> **tcn-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
tcn-guard <**true	false**>	Enables or disables TCN-guard on a port. The value could be **true** or **false**. • **true**: enables TCN-guard. • **false**: disables TCN-guard. By default, TCN-guard is disabled.

Usage Guidelines

TCN BPDU is generated when the switch detects a change in the spanning tree topology. If the switch receives many TCN BPDUs in a short period of time, the spanning tree recalculates frequently, causing a large burden on the device and affecting the stability of the network.

After the TCN guard function is enabled, the switch processes only a certain number of topology change packets in a certain period.

Example

- Enable TCN guard on the port ge-1/1/1 for MSTP mode.

```
admin@Xorplus# set protocols spanning-tree mstp interface ge-1/1/1 tcn-guard true
admin@Xorplus# commit
```

set protocols spanning-tree mstp max-age

The **set protocols spanning-tree mstp max-age** command sets the BPDU aging time on the switching device when MSTP is running.

Command Syntax

set protocols spanning-tree mstp max-age <*max-age*>

Parameter

Parameter	Description
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of a received BPDU packets. If the BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp max-age 15
admin@Xorplus# commit
```

set protocols spanning-tree mstp max-hops

The **set protocols spanning-tree mstp max-hops** command sets the maximum hops of a spanning tree when MSTP is running.

Command Syntax

set protocols spanning-tree mstp max-hops <*max-hops*>

Parameter

Parameter	Description
max-hops <*max-hops*>	Specifies the maximum hops of a spanning tree. The value is an integer that ranges from 6 to 40. The default value is 20.

Usage Guidelines

The maximum number of hops of a spanning tree in an MST region determines the network scale.

An MST BPDU has a field that indicates the number of remaining hops:

- The number of remaining hops in a BPDU sent by the root switching device equals the maximum number of hops.
- The number of remaining hops in a BPDU sent by a non-root switching device equals the maximum number of hops minus the number of hops from the non-root switching device to the root switching device.
- If a switching device receives a BPDU in which the number of remaining hops is 0, the switching device will discard the BPDU.

Example

- Set the maximum hops of a spanning tree to 15 when MSTP is running.

```
admin@Xorplus# set protocols spanning-tree mstp max-hops 15
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti bridge-priority

The **set protocols spanning-tree mstp msti bridge-priority** command sets the bridge priority for an MSTI of the switching device.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **bridge-priority** <*bridge-priority*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16. Each process supports a maximum of 16 instances.
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device for an MSTI. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority of the switching device to 55 for MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti interface cost

The **set protocols spanning-tree mstp msti interface cost** command configures the path cost of the link on a physical port or a LAG port for an MSTI.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **interface** <*interface-name*> **cost** <*cost-value*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16.
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
cost <*cost-value*>	Specifies the path cost of an interface. The value is an integer ranges from 0 to 200000000. The default value is 0.

Example

- Set the path cost of ge-1/1/1 to 556 for MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 interface ge-1/1/1 cost 556
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti interface port-priority

The **set protocols spanning-tree mstp msti interface port-priority** command configures the port priority for an MSTI.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **interface** <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16.
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Set the bridge priority of interface ge-1/1/1 to 55 for MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 interface ge-1/1/1 port-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree mstp msti vlan

The **set protocols spanning-tree mstp vlan** command adds a VLAN to an MSTI.

Command Syntax

set protocols spanning-tree mstp msti <*instance-id*> **vlan** <*vlan-id*>

Parameter

Parameter	Description
msti <*instance-id*>	Specifies the MST instance. The value is an integer that ranges from 1 to 16.
vlan <*vlan-id*>	Specifies the bridge priority of the switching device for an MSTI. The value is an integer ranges from 1 to 4094. e.g. 2,3,5-100.

Usage Guidelines

The MSTIs are independent of each other, and the MSTI can correspond to one or more VLANs. However, a VLAN can only correspond to one MSTI. By default, all VLANs in the MST region are mapped to instance 0.

Example

- Add VLAN 100 to MSTI 5.

```
admin@Xorplus# set protocols spanning-tree mstp msti 5 vlan 100
admin@Xorplus# commit
```

set protocols spanning-tree mstp revision-level

The **set protocols spanning-tree mstp revision-level** command sets the revision level of the MST region.

Command Syntax

set protocols spanning-tree mstp revision-level <*level*>

Parameter

Parameter	Description
revision-level <*level*>	Specifies the revision level of the MST region. The value is an integer that ranges from 0 to 65535. The default value is 0.

Usage Guidelines

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST configuration name
- Mappings between MSTIs and VLANs
- MST region revision level

MSTP is a standard protocol, the MSTP revision level of a switching device is 0 by default. If the revision level of some devices from a specified manufacturer is not 0, you must change the MSTP revision level of devices to be the same to compatible with the spanning tree calculation in an MST region.

Example

- Set the MSTP revision level of the switching device to 5.

```
admin@Xorplus# set protocols spanning-tree mstp revision-level 5
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface bpdu-guard

The **set protocols spanning-tree pvst interface bpdu-guard** command configures BPDU-guard on a physical port or a LAG port for Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree pvst interface** <*interface-name*> **bpdu-guard** true command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** commands manually.

Example

- Enable BPDU-guard on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface manual-forwarding

The **set protocols spanning-tree pvst interface manual-forwarding** command manually configures a physical port or a LAG port as a forwarding port for Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **manual-forwarding** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
manual-forwarding <**true	false**>	Manually configure a physical port or a LAG port as a forwarding port. The value could be **true** or **false**. • **true**: manually configures a physical port or a LAG port as a forwarding port. • **false**: disables manual forwarding on a port. By default, manual forwarding is disabled.

Usage Guidelines

After manually configuring a physical port or a LAG port as a forwarding port, the state of the port is always forwarding, unless the port is down. The port does not participate in spanning tree calculation and does not send and receive BPDUs.

Example

- Configure the port ge-1/1/1 as a forwarding port manually for Rapid-PVST+ mode.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 manual-forwarding true
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface mode

The **set protocols spanning-tree pvst interface mode** command configures the link type of a port for Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point**	**shared**>	Specifies the link type of the port. The value could be **point-to-point** or **shared**. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree pvst interface root-guard

The **set protocols spanning-tree pvst interface root-guard** command is used to enable or disable root guard function for Rapid-PVST+.

Command Syntax

set protocols spanning-tree pvst interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
root-guard <**true**	**false**>	Enables or disables root guard function for Rapid-PVST+. The value could be **true** or **false**. • **true**: enables root guard function for Rapid-PVST+. • **false**: disables root guard function for Rapid-PVST+. By default, root guard function is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for Rapid-PVST+ mode on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree pvst interface ge-1/1/1 root-guard true
```

set protocols spanning-tree pvst vlan bridge-priority

The **set protocols spanning-tree pvst vlan bridge-priority** command sets the bridge priority the switching device when Rapid-PVST+ is running.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **bridge-priority** <*bridge-priority*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094. A total of 64 VLANs can be enabled for Rapid-PVST+.
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device for Rapid-PVST+ mode. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 for Rapid-PVST+.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan enable

The **set protocols spanning-tree pvst vlan enable** command is used to enable or disable Rapid-PVST+ VLAN instance.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **enable** <**true | false**>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
enable <**true	false**>	Enables or disables Rapid-PVST+ VLAN instance. The value could be **true** or **false**. • **true**: enables Rapid-PVST+ VLAN instance. • **false**: disables Rapid-PVST+ VLAN instance. By default, Rapid-PVST+ is disabled.

Usage Guidelines

To enable the Rapid-PVST+ protocol, in addition to setting the spanning tree protocol to 4 by using the **set protocols spanning-tree force-version 4** command, Rapid-PVST+ must be enabled on the VLAN.

Example

- Enable Rapid-PVST+ in VLAN 5.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan forward-delay

The **set protocols spanning-tree pvst vlan forward-delay** command sets the value of the Rapid-PVST+ forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **forward-delay** <*forward-delay*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
forward-delay <*forward-delay*>	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the Rapid-PVST+ forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan hello-time

The **set protocols spanning-tree pvst vlan hello-time** command sets the interval of the switching device to send BPDUs when Rapid-PVST+ is running.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **hello-time** <*hello-time*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when Rapid-PVST+ is running.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan interface path-cost

The **set protocols spanning-tree pvst vlan interface path-cost** command configures the link path cost of a physical port or a LAG port in Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **interface** <*interface-name*> **path-cost** <*cost-value*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
interface <*interface-name*>	Specifies a interface name. The value is a string that can be set to a physical port name or a LAG port.
path-cost <*cost-value*>	Specifies the path cost of an interface. The value is an integer ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Path cost to the root bridge. It is determined by the distance between the port sending the configuration BPDU and the root bridge. Smallest root path cost is used as the root port on a non-root bridge. On the root bridge, the path cost of each port is 0.

Example

- Set the path cost of the switching device to 55 for VLAN 5.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 interface ge-1/1/1 path-cost 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan interface port-priority

The **set protocols spanning-tree pvst vlan interface port-priority** command configures the port priority of an interface in Rapid-PVST+ mode.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **interface** <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

In Rapid-PVST+ spanning tree calculation, the port path cost, bridge ID of the sending switch, and port priority determine whether the port can be selected as the designated port. A smaller priority value indicates higher probability of becoming the designated port, and a larger priority value indicates higher probability of becoming the blocking port.

On a network running Rapid-PVST+, a port can function as different roles in different spanning trees so that traffic from different VLANs is forwarded through different physical paths.

Example

- Set the port priority of the switching device to 55 for VLAN 5.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 interface ge-1/1/1 port-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree pvst vlan max-age

The **set protocols spanning-tree pvst vlan max-age** command sets the BPDU aging time on the switching device when Rapid-PVST+ is running.

Command Syntax

set protocols spanning-tree pvst vlan <*vlan-id*> **max-age** <*max-age*>

Parameter

Parameter	Description
vlan <*vlan-id*>	Specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of the BPDU packets. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when Rapid-PVST+ is running.

```
admin@Xorplus# set protocols spanning-tree pvst vlan 5 max-age 15
admin@Xorplus# commit
```

set protocols spanning-tree rstp bridge-priority

The **set protocols spanning-tree rstp bridge-priority** command sets the bridge priority the switching device when RSTP is running.

Command Syntax

set protocols spanning-tree rstp bridge-priority <*bridge-priority*>

Parameter

Parameter	Description
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device when RSTP is running. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 when RSTP is running.

```
admin@Xorplus# set protocols spanning-tree rstp bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree rstp forward-delay

The **set protocols spanning-tree rstp forward-delay** command sets the value of the RSTP forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree rstp forward-delay <*forward-delay*>

Parameter

Parameter	Description
forward-delay <*forward-delay*>	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the RSTP forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree rstp forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree rstp hello-time

The **set protocols spanning-tree rstp hello-time** command sets the interval of the switching device to send BPDUs when RSTP is running.

Command Syntax

set protocols spanning-tree rstp hello-time <*hello-time*>

Parameter

Parameter	Description
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when RSTP is running.

```
admin@Xorplus# set protocols spanning-tree rstp hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface bpdu-filter

The **set protocols spanning-tree rstp interface bpdu-filter** command configures a physical port or a LAG port as a BPDU-filter port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **bpdu-filter** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-filter <**true	false**>	Enables or disables BPDU-filter on a port. The value could be **true** or **false**. • **true**: enables BPDU-filter. • **false**: disables BPDU-filter. By default, BPDU-filter is disabled.

Usage Guidelines

When configuring a port as a BPDU-filter port, the port will not process BPDUs.

NOTE:

If the port is set to the BPDU filter port, the port does not participate in spanning tree calculation, so it is recommended to configuring BPDU-filter port only on edge ports.

Example

- Configure the port ge-1/1/1 as a BPDU-filter port.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 bpdu-filter true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface bpdu-guard

The **set protocols spanning-tree rstp interface bpdu-guard** command configures a physical port or a LAG port as a BPDU-guard port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree pvst interface** <*interface-name*> **bpdu-guard true** command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** commands manually.

Example

- Configure the port ge-1/1/1 as a BPDU-guard port.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface edge

The **set protocols spanning-tree rstp interface edge** command configures a physical port or a LAG port as an edge port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **edge** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
edge <**true	false**>	Enables or disables edge on a port. The value could be **true** or **false**. • **true**: enables a physical or a LAG port as an edge port. • **false**: disables a physical or a LAG port as an edge port. By default, edge port is disabled.

Usage Guidelines

The edge port does not participate in the spanning tree calculation. However, once the edge port receives a configuration BPDU, the switching device automatically sets the edge port to a non-edge port and performs spanning tree calculation again.

Example

- Configure the port ge-1/1/1 as an edge port.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 edge true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface mode

The **set protocols spanning-tree rstp interface mode** command configures the link type of the port.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point**	**shared**>	Specifies the link type of the port. The value could be **point-to-point** or shared. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface path-cost

The **set protocols spanning-tree rstp interface path-cost** command configures the link path cost of a physical port or a LAG port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
path-cost <*path-cost*>	Specifies the path cost value of the external link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Path cost to the root bridge. It is determined by the distance between the port sending the configuration BPDU and the root bridge. Smallest root path cost is used as the root port on a non-root bridge. On the root bridge, the path cost of each port is 0.

Example

- Configure the path cost of port ge-1/1/1 to 500.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 path-cost 500
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface port-priority

The **set protocols spanning-tree rstp interface port-priority** command configures the priority of a port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Configure the port priority of ge-1/1/1 to 15.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 port-priority 15
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface root-guard

The **set protocols spanning-tree rstp interface root-guard** command is used to enable or disable root guard function for RSTP.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name.
root-guard <**true**	**false**>	Enables or disables root guard function for RSTP. The value could be **true** or **false**. • **true**: enables root guard function for RSTP. • **false**: disables root guard function for RSTP. By default, root guard function for RSTP is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for RSTP on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 root-guard true
admin@Xorplus# commit
```

set protocols spanning-tree rstp interface tcn-guard

The **set protocols spanning-tree rstp interface tcn-guard** command configures TCN (Topology Change Notification) guard on a physical port or a LAG port for RSTP mode.

Command Syntax

set protocols spanning-tree rstp interface <*interface-name*> **tcn-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
tcn-guard <**true	false**>	Enables or disables TCN-guard on a port. The value could be **true** or **false**. • **true**: enables TCN-guard. • **false**: disables TCN-guard. By default, TCN-guard is disabled.

Usage Guidelines

TCN BPDU is generated when the switch detects a change in the spanning tree topology. If the switch receives many TCN BPDUs in a short period of time, the spanning tree recalculates frequently, causing a large burden on the device and affecting the stability of the network.

After the TCN guard function is enabled, the switch processes only a certain number of topology change packets in a certain period.

Example

- Enable TCN guard on the port ge-1/1/1 for RSTP mode.

```
admin@Xorplus# set protocols spanning-tree rstp interface ge-1/1/1 tcn-guard true
admin@Xorplus# commit
```

set protocols spanning-tree rstp max-age

The **set protocols spanning-tree rstp max-age** command sets the BPDU aging time on the switching device when RSTP is running.

Command Syntax

set protocols spanning-tree rstp max-age <*max-age*>

Parameter

Parameter	Description
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of the BPDU packets. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when RSTP is running.

```
admin@Xorplus# set protocols spanning-tree rstp max-age 15
admin@Xorplus# commit
```

set protocols spanning-tree stp bridge-priority

The **set protocols spanning-tree stp bridge-priority** command sets the bridge priority the switching device when STP is running.

Command Syntax

set protocols spanning-tree stp bridge-priority <*bridge-priority*>

Parameter

Parameter	Description
bridge-priority <*bridge-priority*>	Specifies the bridge priority of the switching device when STP is running. The value is an integer ranges from 0 to 61440. The default value is 32768.

Usage Guidelines

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge. The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

Example

- Set the bridge priority the switching device to 55 when STP is running.

```
admin@Xorplus# set protocols spanning-tree stp bridge-priority 55
admin@Xorplus# commit
```

set protocols spanning-tree stp forward-delay

The **set protocols spanning-tree stp forward-delay** command sets the value of the STP forward delay interval of a switching device.

Command Syntax

set protocols spanning-tree stp forward-delay <*forward-delay*>

Parameter

Parameter	Description
forward-delay <*forward-delay*>	Specifies the value of the Forward Delay. The value is an integer, in seconds, that ranges from 4 to 30. The default value 15s.

Usage Guidelines

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the value of the STP forward delay interval of a switching device to 20s.

```
admin@Xorplus# set protocols spanning-tree stp forward-delay 20
admin@Xorplus# commit
```

set protocols spanning-tree stp hello-time

The **set protocols spanning-tree stp hello-time** command sets the interval of the switching device to send BPDUs when STP is running.

Command Syntax

set protocols spanning-tree stp hello-time <*hello-time*>

Parameter

Parameter	Description
hello-time <*hello-time*>	Specifies the interval of the switch to send BPDUs. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 2s.

Usage Guidelines

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 * (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 * (Hello Time + 1.0)

Example

- Set the interval of the switching device to send BPDUs to 5s when STP is running.

```
admin@Xorplus# set protocols spanning-tree stp hello-time 5
admin@Xorplus# commit
```

set protocols spanning-tree stp interface bpdu-filter

The **set protocols spanning-tree stp interface bpdu-filter** command configures a physical port or a LAG port as a BPDU-filter port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **bpdu-filter** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-filter <**true	false**>	Enables or disables BPDU-filter on a port. The value could be **true** or **false**. • **true**: enables BPDU-filter. • **false**: disables BPDU-filter. By default, BPDU-filter is disabled.

Usage Guidelines

When configuring a port as a BPDU-filter port, the port will not process BPDUs.

NOTE:

If the port is set to the BPDU filter port, the port does not participate in spanning tree calculation, so it is recommended to configuring BPDU-filter port only on edge ports.

Example

- Configure the port ge-1/1/1 as a BPDU-filter port.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 bpdu-filter true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface bpdu-guard

The **set protocols spanning-tree stp interface bpdu-guard** command configures a physical port or a LAG port as a BPDU-guard port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **bpdu-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
bpdu-guard <**true	false**>	Enables or disables BPDU-guard on a port. The value could be **true** or **false**. • **true**: enables BPDU-guard. • **false**: disables BPDU-guard. By default, BPDU-guard is disabled.

Usage Guidelines

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **set protocols spanning-tree pvst interface** <*interface-name*> **bpdu-guard true** command to configure BPDU guard on a switching device.

After BPDU guard is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. To restore the interface, run the **set interface gigabit-ethernet** <*interface-name*> **disable false** commands manually.

Example

- Configure the port ge-1/1/1 as a BPDU-guard port.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 bpdu-guard true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface edge

The **set protocols spanning-tree stp interface edge** command configures a physical port or a LAG port as an edge port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **edge** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
edge <**true	false**>	Enables or disables edge on a port. The value could be **true** or **false**. • **true**: enables a physical or a LAG port as an edge port. • **false**: disables a physical or a LAG port as an edge port. By default, edge port is disabled.

Usage Guidelines

The edge port does not participate in the spanning tree calculation. However, once the edge port receives a configuration BPDU, the switching device automatically sets the edge port to a non-edge port and performs spanning tree calculation again.

Example

- Configure the port ge-1/1/1 as an edge port.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 edge true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface mode

The **set protocols spanning-tree stp interface mode** command configures the link type of the port.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **mode** <**point-to-point** | **shared**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
mode <**point-to-point**	**shared**>	Specifies the link type of the port. The value could be **point-to-point** or **shared**. • **point-to-point**: specifies the current Ethernet port to work in full-duplex mode to achieve fast convergence. • **shared**: specifies the current Ethernet port to work in half-duplex mode. The default value is **point-to-point**.

Example

- Configure the link type of port ge-1/1/1 to **point-to-point**.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 mode point-to-point
admin@Xorplus# commit
```

set protocols spanning-tree stp interface path-cost

The **set protocols spanning-tree stp interface path-cost** command configures the link path cost of a physical port or a LAG port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **path-cost** <*path-cost*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
path-cost <*path-cost*>	Specifies the path cost value of the external link. The value is an integer that ranges from 0 to 200000000. The default value is 0.

Usage Guidelines

Path cost to the root bridge. It is determined by the distance between the port sending the configuration BPDU and the root bridge. Smallest root path cost is used as the root port on a non-root bridge. On the root bridge, the path cost of each port is 0.

Example

- Configure the path cost of the external link on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 path-cost 500
admin@Xorplus# commit
```

set protocols spanning-tree stp interface port-priority

The **set protocols spanning-tree stp interface port-priority** command configures the priority of a port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **port-priority** <*port-priority*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
port-priority <*port-priority*>	Specifies the priority value of a port. The value is an integer that ranges from 0 to 240. The default value is 128.

Usage Guidelines

The value of the port priority affects whether the port will be elected as the designated port. The smaller the priority value is, the higher the priority is, and it is more likely to become the designated port.

Example

- Configure the port priority of ge-1/1/1 to 15.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 port-priority 15
admin@Xorplus# commit
```

set protocols spanning-tree stp interface root-guard

The **set protocols spanning-tree stp interface root-guard** command is used to enable or disable root guard function for STP.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **root-guard** <**true** | **false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name.
root-guard <**true** | **false**>	Enables or disables root guard function for STP. The value could be **true** or **false**. • **true**: enables root guard function for STP. • **false**: disables root guard function for STP. By default, root guard function for STP is disabled.

Usage Guidelines

If a port is enabled with the root guard function, its port role on all instances can only be the designated port. Once the port that is enabled with root guard receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority for a long time, the port automatically returns to the Forwarding state.

Example

- Enable root guard function for STP on port ge-1/1/1.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 root-guard true
admin@Xorplus# commit
```

set protocols spanning-tree stp interface tcn-guard

The **set protocols spanning-tree stp interface tcn-guard** command configures TCN (Topology Change Notification) guard on a physical port or a LAG port for STP mode.

Command Syntax

set protocols spanning-tree stp interface <*interface-name*> **tcn-guard** <**true | false**>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies a port name. The value is a string that can be set to a physical port name or a LAG port.
tcn-guard <**true	false**>	Enables or disables TCN-guard on a port. The value could be **true** or **false**. • **true**: enables TCN-guard. • **false**: disables TCN-guard. By default, TCN-guard is disabled.

Usage Guidelines

TCN BPDU is generated when the switch detects a change in the spanning tree topology. If the switch receives many TCN BPDUs in a short period of time, the spanning tree recalculates frequently, causing a large burden on the device and affecting the stability of the network.

After the TCN guard function is enabled, the switch processes only a certain number of topology change packets in a certain period.

Example

- Enable TCN guard on the port ge-1/1/1 for STP mode.

```
admin@Xorplus# set protocols spanning-tree stp interface ge-1/1/1 tcn-guard true
admin@Xorplus# commit
```

set protocols spanning-tree stp max-age

The **set protocols spanning-tree stp max-age** command sets the BPDU aging time on the switching device when STP is running.

Command Syntax

set protocols spanning-tree stp max-age <*max-age*>

Parameter

Parameter	Description
max-age <*max-age*>	Specifies the BPDU aging time. The value is an integer, in seconds, that ranges from 6 to 40. The default value is 20s.

Usage Guidelines

Max Age is the maximum lifetime of the BPDU packets. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs.

NOTE:

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, network flapping occurs.

- 2 x (Forward Delay - 1.0) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0)

Example

- Set BPDU aging time to 15s when STP is running.

```
admin@Xorplus# set protocols spanning-tree stp max-age 15
admin@Xorplus# commit
```

MLAG Commands

- set protocols mlag domain
- set protocols mlag domain node
- set protocols mlag domain interface link
- set protocols mlag domain peer-ip peer-link
- set protocols mlag domain peer-ip peer-vlan
- run show mlag domain
- run show mlag link
- run show mlag consistency-parameter

set protocols mlag domain

The **set protocols mlag domain** command creates an MLAG domain ID.

Command Syntax

set protocols mlag domain <*domain-id*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.

Example

- Create an MLAG domain.

```
admin@Xorplus# set protocols mlag domain 3
```

set protocols mlag domain node

The **set protocols mlag domain node** command specifies the node ID for the MLAG device.

Command Syntax

set protocols mlag domain <*domain-id*> **node** <**0 | 1**>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
node <**0	1**>	Specifies the node ID for the MLAG device. The value could be **0** or **1**.

Example

- Set the node ID for the MLAG device as 0.

```
admin@Xorplus# set protocols mlag domain 3 node 0
```

set protocols mlag domain interface link

The **set protocols mlag domain interface link** command configures the link ID on the MLAG member port.

Command Syntax

set protocols mlag domain <*domain-id*> **interface** <*lag-interface*> **link** <*link-id*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
interface <*lag-interface*>	Specifies the MLAG member port. The value is a LAG interface.
link <*link-id*>	Specifies the link ID. The value is an integer that ranges from 1 to 255.

Example

- Configure the link ID to 2 on MLAG member port ae3.

```
admin@Xorplus# set protocols mlag domain 3 interface ae3 link 2
```

set protocols mlag domain peer-ip peer-link

The **set protocols mlag domain peer-ip peer-link** command configures peer IP address and peer link port.

Command Syntax

set protocols mlag domain <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-link** <*peer-interface-name*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
peer-ip <*peer-ipv4-address*>	The IP address of the remote MLAG peer link port. The value is in dotted decimal notation.
peer-link <*peer-interface-name* >	The interface name of the peer link that is on the peer device, it should be a LAG port.

Example

- Configure peer IP address and peer link port.

```
admin@Xorplus# set interface mlag domain 3 peer-ip 10.10.10.1 peer-link ae1
```

set protocols mlag domain peer-ip peer-vlan

The **set protocols mlag domain peer-ip peer-vlan** command configures an MLAG peer VLAN.

Command Syntax

set protocols mlag domain <*domain-id*> **peer-ip** <*peer-ipv4-address*> **peer-vlan** <*vlan-id*>

Parameters

Parameter	Description
domain <*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
peer-ip <*peer-ipv4-address*>	The IP address of the remote MLAG peer-link port. The value is in dotted decimal notation.
peer-vlan <*vlan-id*>	Specifies a peer VLAN ID. The value is an integer that ranges from 1 to 4094. The recommended value is 4088.

Usage Guidelines

A specified VLAN MUST be assigned to the peer-link interface, the MLAG peer VLAN, which is dedicated to transmitting MLAG control plane messages but does not allow data messages.

Example

- Configure a peer VLAN for MLAG.

```
admin@Xorplus# set l3-interface vlan-interface vlan4088 address 10.10.10.24 prefix-length 24
admin@Xorplus# set protocols mlag domain 2 peer-ip 10.10.10.1 peer-link ae2
admin@Xorplus# set interface mlag domain 2 peer-ip 10.10.10.1 peer-vlan 4088
```

run show mlag domain

The **run show mlag domain** command displays the global MLAG domain information.

Command Syntax

run show mlag domain {<*domain-id*>| **summary**}

Parameter

Parameter	Description
<*domain-id*>	Specifies a domain ID. The value is an integer that ranges from 1 to 255.
summary	Show all MLAG information for all the MLAG domains. Currently, only one domain is supported on one MLAG device.

Example

- Show the global MLAG domain information.

```
admin@Xorplus# run show mlag domain summary
Domain ID: 1    Domain MAC: 48:6E:73:FF:00:01    Node ID: 0
-------------------------------------------------------------------------------------------
Peer Link  Peer IP  Peer Vlan  Neighbor     Status  Config Matched  MAC Synced  # of Links
---------  -------   --------  ---------  ----------    ---------    --------    -------
ae23       1.1.1.2    4088    ESTABLISHED      Yes       Yes                       2
```

Table 1. Description of the run show mlag domain command output

Item	Description
Domain-ID	Indicates the MLAG domain ID.
Domain-MAC	Indicates the MLAG domain MAC of MLAG device.
Node-ID	Indicates Node ID of the local MLAG device.
Peer-Link	Indicates the local peer-link port.
Peer-IP	Indicates IP address of the remote peer-link port.
Peer Vlan	Indicates the MLAG peer VLAN.
Neighbor Status	Indicates MLAG neighbor status, the value could be IDLE, CONNECTING, ESTABLISHED.
Config Matched	Indicates the consistency check results, the value could be **Yes** or **No**. When all the check items in the configuration consistency check list in 1.1.6 Configuration Consistency Check are consistent, including **Global configuration** and **Per MLAG configuration**, then it is displayed as **Yes**, otherwise it is **No**.
MAC Synced	Indicates whether MAC synchronization is performed between the MLAG peer devices, the value could be **Yes** or **No**. When both the following conditions match, it displays **Yes**, indicating that the MLAG MAC Sync function is normal between the two MLAG devices: • When "**Neighbor Status**" is ESTABLISHED; • In the result of **run show mlag consistency-parameter link** <*link-id*>, “Port Configurations” are all PASS, and in the result of **run show mlag consistency-parameter summary**, “MLAG Configurations” are all PASS. If any of the above conditions is not satisfied, **No** is displayed, indicating that MAC sync has stopped between the MLAG peers.
# of Links	Indicates numbers of MLAG.

run show mlag link

The **run show mlag link** command displays MLAG link information.

Command Syntax

run show mlag link {*<link-id>*| **summary**}

Parameter

Parameter	Description
<link-id>	Specifies the MLAG link ID to show the specific MLAG information.
summary	Show MLAG information for all the MLAG links.

Example

- Show the MLAG link information.

```
admin@XorPlus# run show mlag link summary
# of Links: 2
Link   Local LAG   Link Status   Local Status   Peer Status   Config Matched   Flood
----   --------   -----------   ------------   -----------   --------------   -----
1      ae1         IDLE          UP             UNKNOWN       No               No
2      ae2         IDLE          UP             UNKNOWN       No               No
```

Table 1. Description of the run show mlag link command output

Item	Description
Link	Indicates the link ID of each MLAG.
Local LAG	Indicates the MLAG member port number on local MLAG device.
Link Status	Indicates MLAG interface state, the value could be INIT, IDLE, DOWN, STANDBY, AS_DOWN, AS_PEER, AS_LOCAL or FULL.
Local Status	Indicates the status of local MLAG member port, the value could be UP, DOWN or UNKNOWN.
Peer Status	Indicates the status of remote MLAG member port, the value could be UP, DOWN or UNKNOWN.
Config Matched	Indicates the consistency check results, the value could be Yes or No.
Flood	Indicates whether traffic received on the MLAG peer-link cannot be transferred through the MLAG member port. The value could be **Yes** or **No**. • **Yes**: indicates that traffic received on the MLAG peer-link can be transferred through the MLAG member port. This happens only in the case when peer MLAG member port is down, the MLAG interface state changes to AS_LOCAL. • **No**: indicates that traffic received on the MLAG peer-link cannot be transferred through the MLAG member port.

run show mlag consistency-parameter

The **run show mlag consistency-parameter** command displays the result of MLAG configuration consistency check, including the global and per MLAG configuration.

Command Syntax

run show mlag consistency-parameter { **link** <*link-id*>| **summary**}

Parameter

Parameter	Description
link <*link-id*>	Specifies the MLAG link ID. This displays the result of per MLAG configuration consistency check.
summary	Show the result of global MLAG configuration consistency check.

Example

- Show the result of per MLAG configuration consistency check.

```
admin@Xorplus# run show mlag consistency-parameter link 3
Port Configurations:
----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
MTU                     1514             1514             PASS
Mac Learning            Yes              Yes              PASS
Lag Mode                LACP             LACP             PASS
Native Vlan             3                3                PASS
Port Vlan Mode          Access           Access           PASS
Trunk Vlan Count        2                2                PASS
Trunk VLAN IDs                                            PASS

Spanning-Tree Configurations:
----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ------
Mode                    PVST             PVST             PASS
BPDU Guard              No               No               PASS
Root Guard              No               No               PASS
Manual Forwarding       No               No               PASS
Link Type               P2P              P2P              PASS
Instance Count          1                1                PASS
Instance Vlan 3

-- Port Priority        128              128              PASS
-- Path Cost            0                0                PASS

VXLAN Configurations:
----------------------------------------------------------------
Property                Local Value      Peer Value       Result
----------------------  ---------------  ---------------  ----
```

- Show the result of global MLAG configuration consistency check.

```
admin@Xorplus# run show mlag consistency-parameter summary
Overall : PASS
--------------
Global  : PASS
Link 1  : PASS
Link 2  : PASS
```

```
Link 3  : PASS

MLAG Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Domain ID                1                1                PASS
Node ID                  1                0                PASS
Peer VLAN                4088             4088             PASS
Link Count               3                3               PASS
Link IDs                 1   2   3       1   2   3       PASS

Spanning-Tree Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   Yes              Yes              PASS
Mode                     PVST             PVST             PASS
Instance Count           65               65               PASS
Instance Vlan 1
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS
Instance Vlan 2
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS
Instance Vlan 3
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS
Instance Vlan 4
-- Bridge Priority       32768            32768            PASS
-- Hello Time            2                2                PASS
-- Forward Delay         15               15               PASS
-- Max Age               20               20               PASS

DHCP Snooping Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
VLAN Count               0                4                FAIL
VLAN IDs                                                   FAIL

IGMP Snooping Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
Enable                   No               No               PASS

VXLAN Configurations:
----------------------------------------------------------------
Property                 Local Value      Peer Value       Result
-----------------------  ---------------  ---------------  ------
VXLAN                    N/A              N/A              PASS
VXLAN VNI Count          0                0                PASS
VXLAN VNIs                                                 PASS
```

GRE Tunnel Interface Commands

- run show l3-interface tunnel
- set l3-interface tunnel address
- set l3-interface tunnel destination
- set l3-interface tunnel disable
- set l3-interface tunnel source
- set l3-interface tunnel tunnel-mode gre-ip
- set l3-interface tunnel vrf

run show l3-interface tunnel

To display information about an GRE tunnel interface, use the **run show l3-interface tunnel** command in L2/L3 configuration mode.

> **NOTE:**
> GRE tunnel is a logical interface created by Linux kernel on software side. Once created, GRE tunnel stays in "**UP**" state in the display of this show command. Unless it is shut down by CLI command "**set l3-interface tunnel ddd disable**", the state will change to "**DOWN**".

Command Syntax

run show l3-interface tunnel <*tunnel-interface-name*>

Parameters

Parameter	Description
tunnel <*tunnel-interface-name*>	The GRE tunnel interface name.

Example

- The following example displays information about GRE tunnel interface **tnl1**. In the output information, **Inet addr** indicates the tunnel interface IP address.

```
admin@Xorplus# run show l3-interface tunnel tnl1
tnl1        State:UP
            Tunnel Source: 1.1.1.1
            Tunnel Destnation:: 2.2.2.2
            Tunnel protocol/transport: gre-ip
            Inet addr: 10.1.1.1/24
            Traffic statistics:
              5 sec input rate IPv4 0 packets/sec, IPv6 0 packets/sec
              5 sec forwarding rate IPv4 0 packets/sec, IPv6 0 packets/sec
              IPv4 Input Packets.........................0
              IPv4 Forwarding Packets....................0
              IPv6 Input Packets.........................0
              IPv6 Forwarding Packets....................0
```

set l3-interface tunnel address

Run the command **set l3-interface tunnel address** to configure a GRE tunnel name and tunnel interface IP address.

Use the command **delete-interface tunnel address** to delete this tunnel from the switch configuration.

> **NOTEs:**
> Note that before committing this configuration, make sure you have configured the tunnel mode as **gre-ip** by using the command **set l3-interface tunnel tunnel-mode.**

Command Syntax

set l3-interface tunnel <*tunnel-name*> **address** <*ip-address*> **prefix-length** <*prefix-length*>

delete l3-interface tunnel <*tunnel-name*> **address** <*ip-address*> **prefix-length** <*prefix-length*>

Parameter

Parameter	Description
tunnel <*tunnel-name*>	Specifies the tunnel name, in alpha-numeric format with no spaces.
address <*ip-address*>	Specifies the tunnel interface IPv4 or IPv6 address.
prefix-length <*prefix-length*>	Specifies the IP prefix length.

Example

- Create a GRE tunnel tn14 and assign 192.168.8.1 as the tunnel interface address with prefix length 24.

```
admin@switch1# set l3-interface tunnel tnl4 address 192.168.8.1 prefix-length 24
admin@switch1# set l3-interface tunnel tnl4 tunnel-mode gre-ip
admin@switch1# commit
```

set l3-interface tunnel destination

Run the command **set l3-interface tunnel destination** to configure the GRE tunnel destination IPv4 address.

Run the command **delete l3-interface tunnel destination** to delete this configuration.

Command Syntax

set l3-interface tunnel <*tunnel-name***> destination <***IPv4-address***>**

delete l3-interface tunnel <*tunnel-name***> destination <***IPv4-address***>**

Parameter

Parameter	Description
tunnel <*tunnel-name***>**	Specifies the name of the tunnel, its value is alpha-numeric with no spaces.
destination <*IPv4-address***>**	Specifies the GRE tunnel destination IP address in IPv4 format.

Example

- Configure the destination GRE tunnel IPv4 address for tunnel tnl4.

```
admin@XorPlus# set l3-interface tunnel tnl4 destination 1.1.1.1
admin@Xorplus# commit
```

set l3-interface tunnel disable

The **set l3-interface tunnel disable** command can be used to enable or disable a GRE tunnel interface.

Command Syntax

set l3-interface tunnel <*tunnel-interface-name*> **disable** <**true | false**>

Parameters

Parameter	Description
tunnel <*tunnel-interface-name*>	Specifies the name of the GRE tunnel interface. The value is a string.
disable <**true	false**>	Enables or disables the GRE tunnel interface. The value could be **true** or **false**. • **true**: Disable the GRE tunnel interface. • **false**: Enable the GRE tunnel interface. When a GRE tunnel interface is created, it is enabled by default.

Example

- Disable GRE tunnel interface tl2.

```
admin@Xorplus# set l3-interface tunnel tl2 disable true
admin@Xorplus# commit
```

set l3-interface tunnel source

Run the command **set l3-interface tunnel source** to configure the GRE tunnel source IPv4 address or source interface.

Run the command **delete l3-interface tunnel source** to delete this configuration.

Command Syntax

set l3-interface tunnel <*tunnel-name***> source** <*tunnel-source*>

delete l3-interface tunnel <*tunnel-name***> source** <*tunnel-source*>

Parameter

Parameter	Description
tunnel <*tunnel-name***>**	Specifies the name of the GRE tunnel in alpha-numeric format with no spaces.
source <*tunnel-source*>	Specifies the GRE tunnel source IPv4 address or source interface. PicOS supports to configure a loopback interface, an L3 VLAN interface, a routed interface or a sub-interface to a GRE tunnel. If multiple IP addresses are configured on the source interface, the smallest IP address will be the source IP address of this GRE tunnel.

Example

- Configure the GRE tunnel source IPv4 address as 2.2.2.2 for tunnel tnl4.

```
admin@XorPlus# set l3-interface tunnel tnl4 source 2.2.2.2
admin@Xorplus# commit
```

set l3-interface tunnel tunnel-mode gre-ip

Run the command **set l3-interface tunnel tunnel-mode gre-ip** to configure the tunnel mode. Currently only GRE tunnel type is supported by PICOS.

To delete this configuration, run the command **delete l3-interface tunnel tnl4 tunnel-mode gre-ip.**

Command Syntax

set l3-interface tunnel <*tunnel-name*> **tunnel-mode gre-ip**

delete l3-interface tunnel <*tunnel-name*> **tunnel-mode gre-ip**

Parameter

Parameter	Description
tunnel <*tunnel-name*>	Specifies the tunnel name, in alpha numeric format with no spaces.

Example

- Set the tunnel mode of tunnel tnl4 to gre-ip.

```
admin@XorPlus# set l3-interface tunnel tnl4 tunnel-mode gre-ip
admin@Xorplus# commit
```

set l3-interface tunnel vrf

Run the command **set l3-interface tunnel vrf vrf1** to configure the VRF for the GRE tunnel to attach to.

Run the command **delete l3-interface tunnel vrf vrf1** to delete this configuration.

Command Syntax

set l3-interface tunnel <*tunnel-name*> **vrf** <*vrf-name*>

delete l3-interface tunnel <*tunnel-name***> vrf** <*vrf-name*>

Parameter

Parameter	Description
vrf <*vrf-name*>	Specifies the name of the VRF for the GRE tunnel to attach to.
tunnel <*tunnel-name*>	Specifies the GRE tunnel name in alpha-numeric format with no spaces.

Example

- Configure the VRF vrf1 for the GRE tunnel tnl4.

```
admin@XorPlus# set l3-interface tunnel tnl4 vrf vrf1
admin@Xorplus# commit
```

GVRP Commands

- set protocols gvrp join-timer
- set protocols gvrp leave-timer
- set protocols gvrp leaveall-timer
- run clear gvrp interface statistics
- run show gvrp interface
- run show gvrp interface statistics
- set protocols gvrp edge-switch
- set protocols gvrp enable
- set protocols gvrp interface enable
- set protocols gvrp traceoptions flag config
- set protocols gvrp traceoptions flag packets

set protocols gvrp join-timer

The **set protocols gvrp join-timer** command configures the join timer duration for GVRP.

The **delete protocols gvrp join-timer** command deletes the configuration.

> **NOTE**s:
> It is highly recommended to KEEP the default configuration of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

Command Syntax

set protocols gvrp join-timer *<join-timer>*

delete protocols gvrp join-timer

Parameter

Parameter	Description
<join-timer>	Specifies the join timer. The value is an integer in milliseconds that ranges from 100 to 500. The default value is 200 milliseconds.

Example

- Configure the join timer.

```
admin@PICOS# set protocols gvrp join-timer 300
admin@PICOS# commit
```

set protocols gvrp leave-timer

The **set protocols gvrp leave-timer** command configures the leave timer duration for GVRP.

The **delete protocols gvrp leave-timer** command deletes the configuration.

NOTEs:

It is highly recommended to KEEP the default configuration of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

Command Syntax

set protocols gvrp leave-timer <*leave-timer*>

delete protocols gvrp leave-timer

Parameter

Parameter	Description
<*leave-timer*>	Specifies the leave timer. The value is an integer in milliseconds that ranges from 300 to 1000. The default value is 1000 milliseconds.

Example

- Configure the leave timer.

```
admin@PICOS# set protocols gvrp leave-timer 800
admin@PICOS# commit
```

set protocols gvrp leaveall-timer

The **set protocols gvrp leaveall-timer** command configures the leaveall timer duration for GVRP.

The **delete protocols gvrp leaveall-timer** command deletes the configuration.

NOTEs:

It is highly recommended to KEEP the default configuration of GVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of GVRP.

Command Syntax

set protocols gvrp leaveall-timer *<leaveall-timer>*

delete protocols gvrp leaveall-timer

Parameter

Parameter	Description
<leaveall-timer>	Specifies the leaveall timer. The value is an integer in seconds that ranges from 10 to 60. The default value is 10 seconds.

Example

- Configure the leaveall timer.

```
admin@PICOS# set protocols gvrp leaveall-timer 50
admin@PICOS# commit
```

run clear gvrp interface statistics

The **run clear gvrp interface statistics** command is used to clear the GVRP packets statistics.

> **NOTE:**
> The previous statistics cannot be restored after clearing, so be careful when using this command.

Command Syntax

run clear gvrp interface <*interface-name*> **statistics**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled GVRP. The value could be a physical interface or a LAG interface.

Example

- Clear the statistics information of GVRP.

```
admin@PICOS# run clear gvrp interface te-1/1/7 statistics
admin@PICOS# run show gvrp interface te-1/1/7 statistics
packet_received: 0
packet_sent:    0
```

run show gvrp interface

The **run show gvrp interface** command is used to view GVRP information on a specific interface, including GVRP Status, Registrar State, Timers and VLANs learned by the interface through GVRP.

Command Syntax

run show gvrp interface *<interface-name>*

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name that enabled GVRP. The value could be a physical interface or a LAG interface.

Example

- View the configuration information of GVRP.

```
admin@PICOS# run show gvrp interface te-1/1/21
Port            Leave Timer(ms)  LeaveAll Timer(s)  Join Timer(ms)
te-1/1/21       1000             10                 200

Port            Vlans Added
te-1/1/21       10, 11
```

run show gvrp interface statistics

The **run show gvrp interface statistics** command is used to view the interface statistics information of GVRP packets on a specific interface.

Command Syntax

run show gvrp interface <*interface-name*> **statistics**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled GVRP. The value could be a physical interface or a LAG interface.

Example

- View the statistics information of GVRP.

```
admin@PICOS# run show gvrp interface te-1/1/21 statistics
packet_received: 245
packet_sent:     248
```

set protocols gvrp edge-switch

The **set protocols gvrp edge-switch** command can be used to enable or disable GVRP edge-switch function.

The **delete protocols gvrp edge-switch** command deletes the configuration.

> **NOTE:**
> This command can be enabled only on the edge switches.

Command Syntax

set protocols gvrp edge-switch <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP edge-switch function. The value could be **true** or **false**. • **true**: Enable GVRP edge-switch function. • **false**: Disable GVRP edge-switch function. By default, GVRP edge-switch function is disabled.

Example

- Enable GVRP edge-switch function.

```
admin@PICOS# set protocols gvrp edge-switch true
admin@PICOS# commit
```

set protocols gvrp enable

The **set protocols gvrp enable** command can be used to enable or disable GVRP function globally.

The **delete protocols gvrp enable** command deletes the configuration.

> **NOTE:**
> To enable GVRP function, users need to enable GVRP BOTH globally and at the per-interface level. The command **set protocols gvrp interface enable** enables GVRP function on a specific interface.

Command Syntax

set protocols gvrp enable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP function globally. The value could be **true** or **false**. • **true**: Enable GVRP function globally. • **false**: Disable GVRP function globally. By default, GVRP function is disabled.

Example

- Enable GVRP function globally.

```
admin@PICOS# set protocols gvrp enable true
admin@PICOS# commit
```

set protocols gvrp interface enable

The **set protocols gvrp interface enable** command can be used to enable or disable GVRP function on a specific interface.

The **delete protocols gvrp interface enable** command deletes the configuration.

> **NOTE:**
> To enable GVRP function, users need to enable GVRP BOTH globally and at the per-interface level. The command **set protocols gvrp enable** enables GVRP function globally.

Command Syntax

set protocols gvrp interface <*interface-name*> **enable** <**true | false**>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface or a LAG interface.
<**true	false**>	Enable or disable GVRP function on a specific interface. The value could be **true** or **false**. • **true**: Enable GVRP function on a specific interface. • **false**: Disable GVRP function on a specific interface. By default, GVRP function is disabled.

Example

- Enable GVRP function on a specific interface.

```
admin@PICOS# set protocols gvrp interface te-1/1/19 enable true
admin@PICOS# commit
```

set protocols gvrp traceoptions flag config

The **set protocols gvrp traceoptions flag config** command can be used to enable or disable GVRP debugging for configuration tracing.

The **delete protocols gvrp traceoptions flag config** command deletes the configuration.

Command Syntax

set protocols gvrp traceoptions flag config disable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable GVRP debugging for configuration tracing. • **false**: Enable GVRP debugging for configuration tracing. By default, GVRP debugging for configuration tracing is disabled.

Example

- Enable GVRP debugging for configuration tracing.

```
admin@PICOS# set protocols gvrp traceoptions flag config disable false
admin@PICOS# commit
```

set protocols gvrp traceoptions flag packets

The **set protocols gvrp traceoptions flag packets** command can be used to enable or disable GVRP debugging for received/sent packets event tracing.

The **delete protocols gvrp traceoptions flag packets** command deletes the configuration.

Command Syntax

set protocols gvrp traceoptions flag packets disable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable GVRP debugging for received/sent packets event tracing. The value could be **true** or **false**. • **true**: Disable GVRP debugging for received/sent packets event tracing. • **false**: Enable GVRP debugging for received/sent packets event tracing. By default, GVRP debugging for received/sent packets event tracing is disabled.

Example

- Enable GVRP debugging for received/sent packets event tracing.

```
admin@PICOS# set protocols gvrp traceoptions flag packets disable false
admin@PICOS# commit
```

MVRP Commands

- run clear mvrp interface statistics
- run show mvrp interface
- run show mvrp interface statistics
- set protocols mvrp edge-switch
- set protocols mvrp enable
- set protocols mvrp interface enable
- set protocols mvrp traceoptions flag config
- set protocols mvrp traceoptions flag packets
- set protocols mvrp join-timer
- set protocols mvrp leave-timer
- set protocols mvrp leaveall-timer

run clear mvrp interface statistics

The **run clear mvrp interface statistics** command is used to clear the MVRP packets statistics.

> **NOTE:**
> The previous statistics cannot be restored after clearing, so be careful when using this command.

Command Syntax

run clear mvrp interface <*interface-name*> **statistics**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled MVRP. The value could be a physical interface or a LAG interface.

Example

- Clear the statistics information of MVRP.

```
admin@PICOS# run clear mvrp interface te-1/1/7 statistics
admin@PICOS# run show mvrp interface te-1/1/7 statistics
packet_received: 0
packet_sent:    0
```

run show mvrp interface

The **run show mvrp interface** command is used to view MVRP information on a specific interface, including MVRP Status, Registrar State, Timers and VLANs learned by the interface through MVRP.

Command Syntax

run show mvrp interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled MVRP. The value could be a physical interface or a LAG interface.

Example

- View the configuration information of MVRP.

```
admin@PICOS# run show mvrp interface te-1/1/21
Port            Leave Timer(ms)  LeaveAll Timer(s)  Join Timer(ms)
te-1/1/21       1000             10                 200

Port            Vlans Added
te-1/1/21       10, 11
```

run show mvrp interface statistics

The **run show mvrp interface statistics** command is used to view the interface statistics information of MVRP packets on a specific interface.

Command Syntax

run show mvrp interface <*interface-name*> **statistics**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name that enabled MVRP. The value could be a physical interface or a LAG interface.

Example

- View the statistics information of MVRP.

```
admin@PICOS# run show mvrp interface te-1/1/21 statistics
packet_received: 245
packet_sent:     248
```

set protocols mvrp edge-switch

The **set protocols mvrp edge-switch** command can be used to enable or disable MVRP edge-switch function.

The **delete protocols mvrp edge-switch** command deletes the configuration.

> **NOTE:**
> This command can be enabled only on the edge switches.

Command Syntax

set protocols mvrp edge-switch <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP edge-switch function. The value could be **true** or **false**. • **true**: Enable MVRP edge-switch function. • **false**: Disable MVRP edge-switch function. By default, MVRP edge-switch function is disabled.

Example

- Enable MVRP edge-switch function.

```
admin@PICOS# set protocols mvrp edge-switch true
admin@PICOS# commit
```

set protocols mvrp enable

The **set protocols mvrp enable** command can be used to enable or disable MVRP function globally.

The **delete protocols mvrp enable** command deletes the configuration.

> **NOTE:**
> To enable MVRP function, users need to enable MVRP BOTH globally and at the per-interface level. The command **set protocols mvrp interface enable** enables MVRP function on a specific interface.

Command Syntax

set protocols mvrp enable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP function globally. The value could be **true** or **false**. • **true**: Enable MVRP function globally. • **false**: Disable MVRP function globally. By default, MVRP function is disabled.

Example

- Enable MVRP function globally.

```
admin@PICOS# set protocols mvrp enable true
admin@PICOS# commit
```

set protocols mvrp interface enable

The **set protocols mvrp interface enable** command can be used to enable or disable MVRP function on a specific interface.

The **delete protocols mvrp interface enable** command deletes the configuration.

> **NOTE:**
> To enable MVRP function, users need to enable MVRP BOTH globally and at the per-interface level. The command **set protocols mvrp enable** enables MVRP function globally.

Command Syntax

set protocols mvrp interface <*interface-name*> **enable** <**true | false**>

Parameters

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface or a LAG interface.
<**true	false**>	Enable or disable MVRP function on a specific interface. The value could be **true** or **false**. • **true**: Enable MVRP function on a specific interface. • **false**: Disable MVRP function on a specific interface. By default, MVRP function is disabled.

Example

- Enable MVRP function on a specific interface.

```
admin@PICOS# set protocols mvrp interface te-1/1/19 enable true
admin@PICOS# commit
```

set protocols mvrp traceoptions flag config

The **set protocols mvrp traceoptions flag config** command can be used to enable or disable MVRP debugging for configuration tracing.

The **delete protocols mvrp traceoptions flag config** command deletes the configuration.

Command Syntax

set protocols mvrp traceoptions flag config disable <true | false>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable MVRP debugging for configuration tracing. • **false**: Enable MVRP debugging for configuration tracing. By default, MVRP debugging for configuration tracing is disabled.

Example

- Enable MVRP debugging for configuration tracing.

```
admin@PICOS# set protocols mvrp traceoptions flag config disable false
admin@PICOS# commit
```

set protocols mvrp traceoptions flag packets

The **set protocols mvrp traceoptions flag packets** command can be used to enable or disable MVRP debugging for received/sent packets event tracing.

The **delete protocols mvrp traceoptions flag packets** command deletes the configuration.

Command Syntax

set protocols mvrp traceoptions flag packets disable <**true | false**>

Parameters

Parameter	Description
<**true	false**>	Enable or disable MVRP debugging for received/sent packets event tracing. The value could be **true** or **false**. • **true**: Disable MVRP debugging for received/sent packets event tracing. • **false**: Enable MVRP debugging for received/sent packets event tracing. By default, MVRP debugging for received/sent packets event tracing is disabled.

Example

- Enable MVRP debugging for received/sent packets event tracing.

```
admin@PICOS# set protocols mvrp traceoptions flag packets disable false
admin@PICOS# commit
```

set protocols mvrp join-timer

The **set protocols mvrp join-timer** command configures the join timer duration for MVRP.

The **delete protocols mvrp join-timer** command deletes the configuration.

> **NOTE**s:
> It is highly recommended to KEEP the default configuration of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

Command Syntax

set protocols mvrp join-timer *<join-timer>*

delete protocols mvrp join-timer

Parameter

Parameter	Description
<join-timer>	Specifies the join timer. The value is an integer in milliseconds that ranges from 100 to 500. The default value is 200 milliseconds.

Example

- Configure the join timer.

```
admin@PICOS# set protocols mvrp join-timer 300
admin@PICOS# commit
```

set protocols mvrp leave-timer

The **set protocols mvrp leave-timer** command configures the leave timer duration for MVRP.

The **delete protocols mvrp leave-timer** command deletes the configuration.

NOTEs:

It is highly recommended to KEEP the default configuration of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

Command Syntax

set protocols mvrp leave-timer *<leave-timer>*

delete protocols mvrp leave-timer

Parameter

Parameter	Description
<leave-timer>	Specifies the leave timer. The value is an integer in milliseconds that ranges from 300 to 1000. The default value is 1000 milliseconds.

Example

- Configure the leave timer.

```
admin@PICOS# set protocols mvrp leave-timer 800
admin@PICOS# commit
```

set protocols mvrp leaveall-timer

The **set protocols mvrp leaveall-timer** command configures the leaveall timer duration for MVRP.

The **delete protocols mvrp leaveall-timer** command deletes the configuration.

> **NOTE**s:
>
> It is highly recommended to KEEP the default configuration of MVRP Timers to ensure the system and network stability. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

Command Syntax

set protocols mvrp leaveall-timer <*leaveall-timer*>

delete protocols mvrp leaveall-timer

Parameter

Parameter	Description
<*leaveall-timer*>	Specifies the leaveall timer. The value is an integer in seconds that ranges from 10 to 60. The default value is 10 seconds.

Example

- Configure the leaveall timer.

```
admin@PICOS# set protocols mvrp leaveall-timer 50
admin@PICOS# commit
```

ERPS Commands

- run show erps brief
- run show erps interface
- run show erps ring
- run show erps statistics
- set protocols erps enable
- set protocols erps ring
- set protocols erps version
- set protocols erps ring instance
- set protocols erps ring instance control-vlan
- set protocols erps ring instance description
- set protocols erps ring instance enable
- set protocols erps ring instance guard-timer
- set protocols erps ring instance holdoff-timer
- set protocols erps ring instance protected-instance
- set protocols erps ring instance r-aps level
- set protocols erps ring instance rpl
- set protocols erps ring instance wtr-timer
- set protocols erps ring port0 interface
- set protocols erps ring port1 interface
- set protocols erps ring r-aps ring-mac
- set protocols erps ring sub-ring
- set protocols erps ring virtual-channel
- set protocols erps ring instance non-revertive
- set protocols erps tcn-propagation
- set protocols erps ring instance connect ring
- erps switch force ring instance
- erps switch manual ring instance
- erps clear ring ring instance
- set protocols erps traceoptions flag all disable
- set protocols erps traceoptions flag config disable
- set protocols erps traceoptions flag ring disable

run show erps brief

The **run show erps brief** command shows brief information of the ERPS configuration.

Command Syntax

run show erps brief

Parameter

None.

Example

- View the brief information of the ERPS configuration.

```
admin@PICOS# run show erps brief
Enable: true
Version: 2
Tcn-propagation: Yes

D: Discarding
F: Forwarding
R: RPL Owner
N: RPL Neighbour
FS: Forced Switch
MS: Manual Switch
Ring ID    Instance ID    Control VLAN    Port0             Port1
------------------------------------------------------------------------------
1          1              4001            te-1/1/19(D,R)    te-1/1/7(F)
2          2              4002            te-1/1/19(F)      te-1/1/7(F)
3          3              4003            te-1/1/19(F)      te-1/1/7(D,R)
```

run show erps interface

The **run show erps interface** command is used to view ERPS interface information, including Port Role, Port State and Signal Failure.

Command Syntax

run show erps interface ring <*ring-id*> **instance** <*instance-id*>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Example

- View ERPS interface information.

```
admin@PICOS# run show erps interface ring 1 instance 1
Interface      Port Role       Port State       Signal Failure
---------------------------------------------------------------
te-1/1/19      RPL Owner       Discarding       Non-failed
te-1/1/7       Common          Forwarding       Non-failed
```

run show erps ring

The **run show erps ring** command shows the detailed information of the ERPS ring instances.

Command Syntax

run show erps ring <*ring-id*> [**instance** <*instance-id*>]

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Optional. Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Example

- View the detailed information of the ERPS ring instances.

```
admin@PICOS# run show erps ring 1
Ring ID: 1
Port0: te-1/1/19
Port1: te-1/1/7
Ring-MAC: false
Sub-ring: No
Virtual-channel: No

Instance ID: 1
Enable: Yes
Active: true
Node state: Protection
Description:
Control VLAN: 4001
Protected instance: 1
Protected VLAN: 100-101,111,4094
Guard timer: 500 ms
Hold-off timer: 0 ms
WTR timer: 1 min
Revertive mode: Revertive
R-APS level : 7
Connect(ring/instance): -
Forced Switch Port: -
Manual Switch Port: -
Interface      Port Role        Port State       Signal Failure
-----------------------------------------------------------------
te-1/1/19      RPL Owner        Forwarding       Non-failed
te-1/1/7       Common           Forwarding       Non-failed


Instance ID: 2
Enable: Yes
Active: true
Node state: Protection
Description:
Control VLAN: 4002
Protected instance: 2
Protected VLAN: 200-201
Guard timer: 500 ms
Hold-off timer: 0 ms
WTR timer: 1 min
Revertive mode: Revertive
R-APS level : 7
```

```
Connect(ring/instance): -
Forced Switch Port: -
Manual Switch Port: -
Interface      Port Role       Port State       Signal Failure
-----------------------------------------------------------------
te-1/1/19      Common          Forwarding       Non-failed
te-1/1/7       Common          Forwarding       Non-failed
```

In the show result,

- The parameter “**Active**” indicates whether the ERPS ring instance is active or not. If the configurations of the ERPS ring instance are correct and complete, the ERPS ring instance is active, and it shows “**Active: true**”.
- The parameter “**Node State**” indicates the state for the node:
  - **Init**: Not a participant of a specific ring.
  - **Idle**: No failure on the ring. Indicates that the current blocking point is at the RPL Owner port.
  - **Protection**: Indicates link failure or equipment fault on the ring.
  - **Pending**: Indicates a transition state for ERPS ring, such as the node is recovering from failure.
  - **Forced Switch**: Indicates that the ERPS ring port is blocked by forced switching.
  - **Manual Switch**: Indicates that the ERPS ring port is blocked by manual switching.

run show erps statistics

The **run show erps statistics** command shows the statistics of ERPS protocol messages sent and received by the ERPS ring ports.

Command Syntax

run show erps statistics [**ring** <*ring-id*> [**instance** <*instance-id*>]]

Parameter

Parameter	Description
ring <*ring-id*>	Optional. Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Optional. Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Example

- View the statistics information of ERPS packets.

```
admin@PICOS# run show erps statistics ring 7
Statistics for ERPS ring 7 instance 1:
R-APS       Port0 Tx     Port0 Rx     Port1 Tx     Port1 Rx
---------   ----------   ----------   ----------   ----------
NR          14           13           14           13
NR,RB       0            1393         0            1
SF          0            0            0            0
MS          0            0            0            0
FS          0            0            0            0
EVENT       6            3            6            9
```

In the show result,

- Rx: Indicates the receiving protocol messages.
- Tx: Indicates the sending protocol messages.
- NR: Indicates the statistics of R-APS (NR) messages.
- NR,RB: Indicates the statistics of R-APS (NR, RB) messages.
- SF: Indicates the statistics of R-APS (SF) messages.
- MS: Indicates the statistics of protocol messages of blocking the port by manual switching.
- FS: Indicates the statistics of protocol messages of blocking the port by forced switching.
- EVENT: Indicates the statistics of Event protocol messages.

set protocols erps enable

The **set protocols erps enable** command can be used to enable or disable ERPS function globally.

The **delete protocols erps enable** command deletes the configuration.

Command Syntax

set protocols erps enable <**true | false**>

delete protocols erps enable

Parameters

Parameter	Description
<**true	false**>	Enable or disable ERPS function globally. The value could be **true** or **false**. • **true**: Enable ERPS function globally. • **false**: Disable ERPS function globally. By default, ERPS function is disabled.

Example

- Enable ERPS function globally.

```
admin@PICOS# set protocols erps enable true
admin@PICOS# commit
```

set protocols erps ring

The **set protocols erps ring** command creates an ERPS ring with a given ID.

The **delete protocols erps ring** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*>

delete protocols erps ring <*ring-id*>

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.

Usage Guidelines

ERPS ring defined in command **set protocols erps ring** <*ring-id*> is a physical ring, however, ring instance can be thought as a logical ring on the physical ring defined in command **set protocols erps ring** <*ring-id*> **instance** <**1 | 2**>. A maximum of eight ERPS rings (including both major ring and sub-ring) are supported on a device, and a maximum of two instances can be configured for each ring.

Example

- Create an ERPS ring with a given ID.

```
admin@PICOS# set protocols erps ring 5
admin@PICOS# commit
```

set protocols erps version

The **set protocols erps version** command configures ERPS version, which could be ERPSv1 or ERPSv2.

The **delete protocols erps version** command restores the configuration to the default value ERPSv2.

Command Syntax

set protocols erps version <1 | 2>

delete protocols erps version

Parameters

Parameter	Description
version <1 | 2>	Specifies ERPS version. The default version is ERPSv2.

Usage Guidelines

PICOS supports both versions of ERPSv1 and ERPSv2. ERPSv2 is fully compatible with ERPSv1 and has the following extensions:

- Sub-ring supporting
- Sub-ring virtual channel/non-virtual channel transmission of RAPS messages
- Manual switching of port blocking, including Forced Switch and Manual Switch
- ERPS ring revertive/non-revertive modes are configurable
- Sub-ring topology change notifications

ERPSv1 only supports major ring networking, while ERPSv2 supports not only major ring, but also supports sub-ring network, and the mixed networking of major ring and sub-ring.

Example

- Configure the ERPS version.

```
admin@PICOS# set protocols erps version 1
admin@PICOS# commit
```

set protocols erps ring instance

The **set protocols erps ring instance** command creates an instance for the ERPS ring.

The **delete protocols erps ring instance** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <**1 | 2**>

delete protocols erps ring <*ring-id*> **instance**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <**1	2**>	Specifies the instance ID for a ring. The value is an integer that could be 1 or 2.

Usage Guidelines

ERPS ring defined in command **set protocols erps ring** <*ring-id*> is a physical ring, however, ring instance can be thought as a logical ring on the physical ring defined in command **set protocols erps ring** <*ring-id*> **instance** <**1 | 2**>. A maximum of eight ERPS rings are supported on a device, and a maximum of two instances can be configured for each ring.

Example

- Create an ERPS ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2
admin@PICOS# commit
```

set protocols erps ring instance control-vlan

The **set protocols erps ring instance control-vlan** command adds a control VLAN to a ring instance.

The **delete protocols erps ring instance control-vlan** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **control-vlan** <*control-vlan*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **control-vlan**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
control-vlan <*control-vlan*>	Specifies the control VLAN ID for a ring instance. The value is an integer that ranges from 1 to 4094.

Usage Guidelines

In an ERPS ring, the control VLAN is used to transmit ERPS protocol packets.

- Each ERPS ring instance must be configured with a control VLAN.
- Different ERPS ring instances cannot use the same control VLAN.
- The same control VLAN must be configured for all devices in the same ERPS ring instance.

Example

- Add a control VLAN to a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 control-vlan 100
admin@PICOS# commit
```

set protocols erps ring instance description

The **set protocols erps ring instance description** command configures the descriptive information to help administrators and operators understand the purpose of a ring instance.

The **delete protocols erps ring instance description** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **description** <*text*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **description**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
description <*text*>	Specifies the descriptive information about the ring instance. The value is a string.

Example

- Configure the descriptive information about the ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 description WestInstance
admin@PICOS# commit
```

set protocols erps ring instance enable

The **set protocols erps ring instance enable** command can be used to enable or disable protection switching on the given instance of the ring. It is disabled by default.

The **delete protocols erps ring instance enable** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **enable** <**true | false**>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **enable**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
enable <**true	false**>	Enable or disable protection switching on the given instance of the ring. The value could be **true** or **false**. • **true**: Enable protection switching on the given instance of the ring. • **false**: Disable protection switching on the given instance of the ring. By default, ERPS ring instance is disabled.

Usage Guidelines

ERPS ring instance can be enabled by the command **set protocols erps ring** <*ring-id*> **instance** <*instance-id*> **enable true**, or by configuring other "**set protocols erps ring** <*ring-id*> **instance** <*instance-id*> xxx" commands in the ERPS CLI.

The command **set protocols erps ring** <*ring-id*> **instance** <*instance-id*> **enable false** can be used to disable ERPS ring instance on the device.

Example

- Enable protection switching on the given instance of the ring.

```
admin@PICOS# set protocols erps ring 5 instance 2 enable true
admin@PICOS# commit
```

set protocols erps ring instance guard-timer

The **set protocols erps ring instance guard-timer** command configures the guard timer duration for a ring instance.

The **delete protocols erps ring instance guard-timer** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **guard-timer** <*guard-timer*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **guard-timer**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
guard-timer <*guard-timer*>	Specifies the guard timer duration of a ring instance. The value is an integer, in milliseconds, that ranges from 10 to 2000. The default value is 500 milliseconds.

Example

- Configure the guard timer duration for a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 guard-timer 300
admin@PICOS# commit
```

set protocols erps ring instance holdoff-timer

The **set protocols erps ring instance holdoff-timer** command configures the holdoff timer for a ring instance.

The **delete protocols erps ring instance holdoff-timer** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **holdoff-timer** <*holdoff-timer*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **holdoff-timer**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
holdoff-timer <*holdoff-timer*>	Specifies the holdoff timer of a ring instance. The value is an integer, in milliseconds, that ranges from 0 to 10000. The default value is 0 millisecond.

Example

- Configure the holdoff timer duration for a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 holdoff-timer 1000
admin@PICOS# commit
```

set protocols erps ring instance protected-instance

The **set protocols erps ring instance protected-instance** command configures the MSTP instance of VLANs that is protected by the ring instance.

The **delete protocols erps ring instance protected-instance** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **protected-instance** <*msti*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **protected-instance**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
protected-instance <*msti*>	Specifies the MSTP instance of VLANs that are protected by this ring instance. The value is an integer that ranges from 1 to 16.

Usage Guidelines

protected-instance <*msti*> is the MSTP instance that are protected by the ring instance, so MSTP instance and VLAN mapping needs to be configured before configure ERPS by using command: **set protocols spanning-tree mstp msti** <*msti*> **vlan** <*vlan-id*>.

Make sure that the control VLAN and data VLANs of the ERPS ring have all been mapped to the MSTP instance.

The traffic of MSTP instance 0 is blocked by ERPS ring.

Multiple protected-instance (protected MSTP instance) can be added to one ERPS instance.

Example

- Configure the MSTP instance that is protected by this ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 protected-instance 6
admin@PICOS# commit
```

set protocols erps ring instance r-aps level

The **set protocols erps ring instance r-aps level** command configures the Automatic Protection Switching (APS) message level for the node on the ERPS ring.

The **delete protocols erps ring instance r-aps level** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **r-aps level** <*level-id*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **r-aps level**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
level <*level-id*>	Specifies the Automatic Protection Switching (APS) message level for the node on the Ethernet ring. The value is an integer that ranges from 1 to 7. The default value of r-aps level is 7.

Usage Guidelines

The default value of r-aps level is 7. All nodes in the ethernet ring must be configured with the same level.

Each ERPS node can only process APS messages with an r-aps level value less than or equal to itself. If a ring port receives an APS message with an R-APS level value larger than its own, all the ring ports belonging to this ERPS instance will become blocking.

Example

- Configure the Automatic Protection Switching (APS) message level for the node.

```
admin@PICOS# set protocols erps ring 5 instance 2 r-aps level 5
admin@PICOS# commit
```

set protocols erps ring instance rpl

The **set protocols erps ring instance rpl** command configures RPL port role for the ERPS ring instance.

The **delete protocols erps ring instance rpl** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **rpl** <**port0** | **port1**> <**owner** | **neighbor**>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **rpl** [<**port0** | **port1**>]

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
<port0 | port1>	Specifies ERPS ring **port0** or **port1**.
<**owner** | **neighbor**>	Specifies RPL port role for the ERPS ring instance. The value could be **owner** or **neighbor**. • **owner**: RPL owner port. • **neighbor**: RPL neighbor port. ERPS ports are ordinary ports if no RPL port role is designated.

Usage Guidelines

Each ERPS ring instance has only one RPL owner port and neighbor port, which are determined by user configuration. By blocking the RPL owner port and neighbor port to forward user traffic, it prevents network loops in the ERPS ring.

Example

- Configure port0 as the RPL owner port for the ERPS ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 rpl port0 owner
admin@PICOS# commit
```

set protocols erps ring instance wtr-timer

The **set protocols erps ring instance wtr-timer** command configures the WTR timer for a ring instance.

The **delete protocols erps ring instance wtr-timer** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **wtr-timer** <*wtr-timer*>

delete protocols erps ring <*ring-id*> **instance** <*instance-id*> **wtr-timer**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
wtr-timer <*wtr-timer*>	Specifies the WTR timer duration of a ring instance. The value is an integer, in minutes, that ranges from 1 to 12. The default value is 5 minutes.

Example

- Configure the WTR timer duration for a ring instance.

```
admin@PICOS# set protocols erps ring 5 instance 2 wtr-timer 5
admin@PICOS# commit
```

set protocols erps ring port0 interface

The **set protocols erps ring port0 interface** command configures port0 of an ERPS ring. An L2 interface in the switch is associated to one of the two member ports (port0 and port1) of an ERPS ring. No more than two ports per node can join the same ERPS ring, which are named ERPS **port0** and **port1**.

The **delete protocols erps ring port0 interface** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **port0 interface** <*interface-name*>

delete protocols erps ring <*ring-id*> **port0 interface**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
interface <*interface-name*>	Specifies port0 interface name of ERPS ring. The value is a physical port.

Example

- Configure port0 of an ERPS ring.

```
admin@PICOS# set protocols erps ring 5 port0 interface ge-1/1/1
admin@PICOS# commit
```

set protocols erps ring port1 interface

The **set protocols erps ring port1 interface** command configures port1 of an ERPS ring. An L2 interface in the switch is associated to one of the two member ports (port0 and port1) of an ERPS ring. No more than two ports per node can join the same ERPS ring, which are named ERPS **port0** and **port1**.

The **delete protocols erps ring port1 interface** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **port1 interface** <*interface-name*>

delete protocols erps ring <*ring-id*> **port1 interface**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
interface <*interface-name*>	Specifies port1 interface name of ERPS ring. The value is a physical port.

Example

- Configure port1 of an ERPS ring.

```
admin@PICOS# set protocols erps ring 5 port1 interface ge-1/1/2
admin@PICOS# commit
```

set protocols erps ring r-aps ring-mac

The **set protocols erps ring r-aps ring-mac** command configure the ring ID as the last byte of the destination MAC address for R-APS packets.

The **delete protocols erps ring r-aps ring-mac** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id*> **r-aps ring-mac**

delete protocols erps ring <*ring-id*> **r-aps ring-mac**

Parameters

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.

Example

- Configure the ERPS ring ID 5 as the last byte of the destination MAC address for R-APS packets.

```
admin@PICOS# set protocols erps ring 5 r-aps ring-mac
admin@PICOS# commit
```

set protocols erps ring sub-ring

The **set protocols erps ring sub-ring** command configures a sub-ring. If not specified, the ring is a major ring.

The **delete protocols erps ring sub-ring** command removes the sub-ring configuration of the ring and sets it to be a major ring. Other sub-ring configurations, such as tcn-propagation function, will no longer take effect.

Command Syntax

set protocols erps ring <*ring-id*> **sub-ring** <**true | false**>

delete protocols erps ring<*ring-id*>**sub-ring**

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
<**true	false**>	Enable or disable ERPS sub-ring. The value could be **true** or **false**. • **true**: Enable ERPS sub-ring. • **false**: Disable ERPS sub-ring. By default, the ERPS ring is a major ring.

Example

- Configure a sub-ring.

```
admin@PICOS# set protocols erps ring 5 sub-ring true
admin@PICOS# commit
```

set protocols erps ring virtual-channel

The **set protocols erps ring virtual-channel** command enables virtual-channel RAPS message transmission method for a sub-ring. By default, the sub-ring RAPS message is transmitted as a non-virtual channel.

The **delete protocols erps ring virtual-channel** command restores the configuration to the default value.

Command Syntax

set protocols erps ring <*ring-id*> **virtual-channel** <**true | false**>

delete protocols erps ring <*ring-id*> **virtual-channel**

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
<**true	false**>	Enable or disable virtual-channel sub-ring RAPS message transmission method. The value could be **true** or **false**. • **true**: Enable virtual-channel sub-ring RAPS message transmission method. • **false**: Disable virtual-channel sub-ring RAPS message transmission method. By default, the sub-ring RAPS message is transmitted as a non-virtual channel.

Usage Guidelines

To enable Virtual-Channel method, the following configurations are required:

1. Enable virtual channel on all the devices of the sub-ring, where the <*ring-id*> is the sub-ring ID.

   set protocols erps ring <*ring-id*> **virtual-channel** <**true | false**>

2. Add the major ring port, which is used for forwarding R-APS messages from the sub-ring, to the control VLAN of the sub-ring.

Example

- Enable virtual-channel RAPS message transmission method for sub-ring 5.

```
admin@PICOS# set protocols erps ring 5 virtual-channel true
admin@PICOS# commit
```

set protocols erps ring instance non-revertive

The **set protocols erps ring instance non-revertive** command configures ERPS non-revertive mode. By default, the ERPS ring is in revertive mode.

The **delete protocols erps ring instance non-revertive** command restores the configuration to the default value, that is, the revertive mode.

Command Syntax

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **non-revertive** <**true | false**>

delete protocols erps ring<*ring-id*>**instance** <*instance-id*> **non-revertive**

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.
<**true	false**>	Enable or disable ERPS non-revertive mode. The value could be **true** or **false**. • **true**: Enable ERPS non-revertive mode. • **false**: Disable ERPS non-revertive mode. By default, ERPS works at revertive mode.

Example

- Configure ERPS non-revertive mode.

```
admin@PICOS# set protocols erps ring 5 instance 2 non-revertive true
admin@PICOS# commit
```

set protocols erps tcn-propagation

The **set protocols erps tcn-propagation** command enables sub-ring topology change notifications. When the topology of the sub-ring changes, the FDB refresh of the port will generate a Topology Change (TC) signal. When the tcn-propagation function is enabled, the intersecting node sends an event flush message to the connect ring when it receives the TC signal.

The **delete protocols erps tcn-propagation** command disables sub-ring topology change notifications.

Command Syntax

set protocols erps tcn-propagation <**true | false**>

delete protocols erps tcn-propagation

Parameter

Parameter	Description
<**true	false**>	Enable or disable topology change notifications. The value could be **true** or **false**. • **true**: Enable sub-ring topology change notifications. • **false**: Disable sub-ring topology change notifications. By default, sub-ring topology change notifications is disabled.

Usage Guidelines

To enable sub-ring topology change notifications, the following configurations are required:

1. Configure the connect ring for a sub-ring on all intersecting nodes.

set protocols erps ring <*ring-id*> **instance** <*instance-id*> **connect ring** <*ring-id*> **instance** <*instance-id*>

2. Enable tcn-propagation function to advertise topology changes to the connect ring on all intersecting nodes.

set protocols erps tcn-propagation <**true | false**>

Example

- Enable sub-ring topology change notifications.

```
admin@PICOS# set protocols erps tcn-propagation true
admin@PICOS# commit
```

set protocols erps ring instance connect ring

The **set protocols erps ring instance connect ring** command configures the connect ring for a sub-ring. Associate a ring with a sub-ring if you want to advertise topology changes in a sub-ring to a ring.

The **delete protocols erps ring instanceconnect ring** command deletes the configuration.

Command Syntax

set protocols erps ring <*ring-id1*> **instance** <*instance-id1*> **connect ring** <*ring-id2*> **instance** <*instance-id2*>

delete protocols erps ring <*ring-id1*> **instance** <*instance-id1*> **connect ring** <*ring-id2*> **instance** <*instance-id2*>

Parameter

Parameter	Description
ring <*ring-id1*>	Specifies the ID of the local sub-ring ID. The value is an integer that ranges from 1 to 8.
instance <*instance-id1*>	Specifies the instance ID for a local sub-ring. The value is an integer that ranges from 1 to 2.
ring <*ring-id2*>	Specifies the ID of the connect ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id2*>	Specifies the instance ID for the connect ring. The value is an integer that ranges from 1 to 2.

Example

- Configure the connect ring 6 for sub-ring 5.

```
admin@PICOS# set protocols erps ring 5 instance 2 connect ring 6 instance 1
admin@PICOS# commit
```

erps switch force ring instance

The **erps switch force ring instance** command configures to block a specific ring instance in the way of force switch in CLI operational mode.

Command Syntax

erps switch force ring <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Usage Guidelines

When configuring this command, pay attention to the following notes:

The command **erps switch force ring** <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**> is an operational mode command which should be executed under the prompt “admin@PICOS>”.

ERPS supports two switching methods to manually configure port blocking:

- **Forced switch**: Ports configured for forced switch are blocked immediately, regardless of whether other links on the ring are faulty or not.
- **Manual switch**: Ports configured for manual switch are blocked if the state of the ring is Idle or Pending, otherwise they are not blocked.

The **run show erps ring** command can be used to show the node state of the ERPS ring instances. If force switch (or manual switch) is set successfully, the ***Node state*** in the show result displays **Forced Switch** (or **Manual Switch**).

The **erps clear ring instance** command can be used to clear the blocking point switching operation of the ERPS ring.

Example

- Configure to block a specific ring instance in the way of force switch.

```
admin@PICOS> erps switch force ring 5 instance 2 port0
```

erps switch manual ring instance

The **erps switch manual ring instance** command configures to block a specific ring instance in the way of manual switch in CLI operational mode.

Command Syntax

erps switch manual ring <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Usage Guidelines

When configuring this command, pay attention to the following notes:

The command **erps switch manual ring** <*ring-id*> **instance** <*instance-id*> <**port0** | **port1**> is an operational mode command which should be executed under the prompt “admin@PICOS>”.

ERPS supports two switching methods to manually configure port blocking:

- **Forced switch**: Ports configured for forced switch are blocked immediately, regardless of whether other links on the ring are faulty or not.
- **Manual switch**: Ports configured for manual switch are blocked if the state of the ring is Idle or Pending, otherwise they are not blocked.

The **run show erps ring** command can be used to show the node state of the ERPS ring instances. If force switch (or manual switch) is set successfully, the ***Node state*** in the show result displays **Forced Switch** (or **Manual Switch**).

The **erps clear ring instance** command can be used to clear the blocking point switching operation of the ERPS ring.

Example

- Configure to block a specific ring instance in the way of manual switch.

```
admin@PICOS> erps switch manual ring 6 instance 1 port1
```

erps clear ring ring instance

The **erps clear ring instance** command is used to clear the blocking point switching operation of the ERPS ring in CLI operational mode.

Command Syntax

erps clear ring <*ring-id*> **instance** <*instance-id*>

Parameter

Parameter	Description
ring <*ring-id*>	Specifies the ID of the ring. The value is an integer that ranges from 1 to 8.
instance <*instance-id*>	Specifies the instance ID for a ring. The value is an integer that ranges from 1 to 2.

Usage Guidelines

When configuring this command, pay attention to the following notes:

The command **erps clear ring ring** <*ring-id*> **instance** <*instance-id*> is an operational mode command which should be executed under the prompt “admin@PICOS>”.

Clear operation is used in the following three cases:

- Clearing the locally configured manual switch and forced switch configurations.
- When the ERPS ring is in the revertive mode, the revert action is triggered manually before the WTB Timer/WTR Timer times out.
- When the ERPS ring is in non-revertive mode, the revert action is triggered manually.

Example

- Configure to clear the blocking point switching operation.

```
admin@PICOS> erps clear ring 6 instance 1
```

set protocols erps traceoptions flag all disable

The **set protocols erps traceoptions flag all disable** command can be used to enable or disable ERPS debugging for tracing all ERPS operations.

The **delete protocols erps traceoptions flag all disable** command deletes the configuration.

Command Syntax

set protocols erps traceoptions flag all disable <**true | false**>

delete protocols erps traceoptions flag all disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable ERPS debugging for tracing all ERPS operations. The value could be **true** or **false**. • **true**: Disable ERPS debugging for tracing all ERPS operations. • **false**: Enable ERPS debugging for tracing all ERPS operations. By default, ERPS debugging for tracing all ERPS operations is disabled.

Example

- Enable ERPS debugging for tracing all ERPS operations.

```
admin@PICOS# set protocols erps traceoptions flag all disable false
admin@PICOS# commit
```

set protocols erps traceoptions flag config disable

The **set protocols erps traceoptions flag config disable** command can be used to enable or disable ERPS debugging for configuration tracing.

The **delete protocols erps traceoptions flag config disable** command deletes the configuration.

Command Syntax

set protocols erps traceoptions flag config disable <**true | false**>

delete protocols erps traceoptions flag config disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable ERPS debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable ERPS debugging for configuration tracing. • **false**: Enable ERPS debugging for configuration tracing. By default, ERPS debugging for configuration tracing is disabled.

Example

- Enable ERPS debugging for configuration tracing.

```
admin@PICOS# set protocols erps traceoptions flag config disable false
admin@PICOS# commit
```

set protocols erps traceoptions flag ring disable

The **set protocols erps traceoptions flag ring disable** command can be used to enable or disable ERPS debugging for all the ERPS tracing except the configuration operation.

The **delete protocols erps traceoptions flag ring disable** command deletes the configuration.

Command Syntax

set protocols erps traceoptions flag ring disable <**true | false**>

delete protocols erps traceoptions flag ring disable

Parameters

Parameter	Description
disable <**true	false**>	Enable or disable ERPS debugging for all the ERPS tracing except the configuration operation. The value could be **true** or **false**. • **true**: Disable ERPS debugging for all the ERPS tracing except the configuration operation. • **false**: Enable ERPS debugging for all the ERPS tracing except the configuration operation. By default, ERPS debugging for all the ERPS tracing except the configuration operation is disabled.

Example

- Enable ERPS debugging for all the ERPS tracing except the configuration operation.

```
admin@PICOS# set protocols erps traceoptions flag ring disable false
admin@PICOS# commit
```

EFM OAM Commands

- set protocols ethernet-oam interface enable
- set protocols ethernet-oam interface mode
- set protocols ethernet-oam interface remote-loopback supported
- set protocols ethernet-oam interface remote-loopback timeout
- ethernet-oam remote-loopback start|stop interface
- set protocols ethernet-oam interface timeout
- set protocols ethernet-oam traceoptions flag packets
- set protocols ethernet-oam traceoptions flag config
- run show ethernet-oam
- run show ethernet-oam statistics

set protocols ethernet-oam interface enable

The **set protocols ethernet-oam interface enable** command can be used to enable or disable EFM OAM function on a specific interface. Note that both ends of the connected OAM link need to be configured with this command to enable the EFM OAM function.

The **delete protocols ethernet-oam interface enable** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **enable** <**true | false**>

delete protocols ethernet-oam interface <*interface-name*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
<**true	false**>	Enable or disable EFM OAM function on a specific interface. The value could be **true** or **false**. • **true**: Enable EFM OAM function on a specific interface. • **false**: Disable EFM OAM function on a specific interface. By default, EFM OAM function is disabled.

Example

- Enable EFM OAM function on a specific interface.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 enable true
admin@PICOS# commit
```

set protocols ethernet-oam interface mode

The **set protocols ethernet-oam interface mode** command configures the EFM OAM mode for the Ethernet port enabled EFM OAM function.

The **delete protocols ethernet-oam interface mode** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **mode** <**active | passive**>

delete protocols ethernet-oam interface <*interface-name*> **mode**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
mode <**active	passive**>	Specifies the EFM OAM mode. The value could be **active** or **passive**. • **Active** mode causes the port to initiate the negotiation process and continually send out EFM OAM information PDUs. • **Passive** mode waits for the peer to initiate the negotiation process. A passive mode port cannot initiate remote loopback activity with the peer. By default, the EFM OAM mode is **active**.

Example

- Configure the EFM OAM mode to **passive** for the Ethernet port enabled EFM OAM.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 mode passive
admin@PICOS# commit
```

set protocols ethernet-oam interface remote-loopback supported

The **set protocols ethernet-oam interface remote-loopback supported** command enables reactions to loopback control OAMPDUs from peers.

The **delete protocols ethernet-oam interface remote-loopback supported** command deletes the configuration.

> **NOTE**:
>
> The responding end has been configured with this command to enable reactions to loopback control OAMPDUs from peers, only after this can the peer end run the command **ethernet-oam remote-loopback start interface** *<interface-name>* to start the EFM OAM remote loopback tests.

Command Syntax

set protocols ethernet-oam interface *<interface-name>* **remote-loopback supported**

delete protocols ethernet-oam interface *<interface-name>* **remote-loopback supported**

Parameter

Parameter	Description
interface *<interface-name>*	Specifies an interface name. The value could be a physical interface, for example, ge-1/1/1, xe-1/1/2, and so on.

Example

- Enable reactions to loopback control OAMPDUs from peers.

```
admin@PICOS# set protocols ethernet-oam interface xe-1/1/2 remote-loopback supported
admin@PICOS# commit
```

set protocols ethernet-oam interface remote-loopback timeout

The **set protocols ethernet-oam interface remote-loopback timeout** command configures the timeout for receiving remote loopback responding message. When times out, the EFM session state falls back to the DISCOVERY phase.

The **delete protocols ethernet-oam interface remote-loopback timeout** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **remote-loopback timeout** <*loopback-timeout*>

delete protocols ethernet-oam interface <*interface-name*> **remote-loopback timeout**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
timeout <*loopback-timeout*>	Specifies the timeout for remote loopback. The value is an integer, in seconds, that ranges from 1 to 10. The default value is 3 seconds.

Example

- Configure the timeout for remote loopback.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 remote-loopback timeout 9
admin@PICOS# commit
```

ethernet-oam remote-loopback start|stop interface

The **ethernet-oam remote-loopback start interface** command starts EFM OAM remote loopback tests on the specific port. The EFM OAM remote loopback control OAMPDU will be sent to the peering device to trigger a remote loopback.

The **ethernet-oam remote-loopback stop interface** command stops EFM OAM remote loopback tests on the specific port. The EFM OAM remote loopback control OAMPDU will be sent to the peering device to stop a remote loopback.The **set protocols dot1x interface authentication-open disable** command enables

Command Syntax

ethernet-oam remote-loopback start interface <*interface-name*>

ethernet-oam remote-loopback stop interface <*interface-name*>

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface, for example, ge-1/1/1, xe-1/1/2, and so on.

Usage Guidelines

When configuring this command, pay attention to the following notes:

- The commands **ethernet-oam remote-loopback start interface** and **ethernet-oam remote-loopback stop interface** are operational mode commands which should be executed under the prompt “admin@PICOS>”.
- Only the **active** mode end can run these two commands to start or stop EFM OAM remote loopback tests.
- Before starting the EFM OAM remote loopback tests, make sure:
  - The EFM OAM connection has been established successfully.
  - Users have to configure command **set protocols ethernet-oam interface** <*interface-name*> **remote-loopback supported** on the responding end to enable reactions to loopback control OAMPDUs from peers.
- EFM OAM remote loopback tests will fail if above conditions are not met. After all of the conditions are met, you need to execute the command **ethernet-oam remote-loopback start interface** <*interface-name*> again to start EFM OAM remote loopback tests again.
- When remote loopback function is implemented, the interface no longer participates in any other Layer 2 or Layer 3 protocols.
- When the remote loopback test is completed, you should use the command **ethernet-oam remote-loopback stop interface** to disable EFM OAM remote loopback tests on the port.
- It is not allowed to modify the EFM OAM mode when remote loopback function is implementing.
- The device sends a Loopback Control OAMPDU to the peer when run command **ethernet-oam remote-loopback start interface** <*interface-name*> or **ethernet-oam remote-loopback stop interface** <*interface-name*>.

Example

- Start EFM OAM remote loopback tests on the specific port.

```
admin@PICOS> ethernet-oam remote-loopback start interface te-1/1/1
```

- Stop EFM OAM remote loopback tests on the specific port.

```
admin@PICOS> ethernet-oam remote-loopback stop interface te-1/1/1
```

set protocols ethernet-oam interface timeout

The **set protocols ethernet-oam interface timeout** command configures the timeout for receiving the EFM OAM protocol messages. When the timeout timer expires, the local OAM entity ages out and terminates its connection with the peer OAM entity.

The **delete protocols ethernet-oam interface timeout** command deletes the configuration.

Command Syntax

set protocols ethernet-oam interface <*interface-name*> **timeout** <*oam-timeout*>

delete protocols ethernet-oam interface <*interface-name*> **timeout**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies an interface name. The value could be a physical interface.
timeout <*oam-timeout*>	Specifies the timeout for receiving EFM protocol messages. The value is an integer, in seconds, that ranges from 2 to 30. The default value is 5 seconds.

Example

- Configure the timeout for receiving EFM protocol messages.

```
admin@PICOS# set protocols ethernet-oam interface te-1/1/19 timeout 10
admin@PICOS# commit
```

set protocols ethernet-oam traceoptions flag packets

The **set protocols ethernet-oam traceoptions flag packets** command can be used to enable or disable EFM OAM debugging for received/sent packets tracing.

The **delete protocols ethernet-oam traceoptions flag packets** command deletes the configuration.

Command Syntax

set protocols ethernet-oam traceoptions flag packets disable <true | false>

delete protocols ethernet-oam traceoptions flag packets

Parameter

Parameter	Description
<**true	false**>	Enable or disable EFM OAM debugging for received/sent packets tracing. The value could be **true** or **false**. • **true**: Disable EFM OAM debugging for received/sent packets tracing. • **false**: Enable EFM OAM debugging for received/sent packets tracing. By default, EFM OAM debugging for received/sent packets tracing is disabled.

Example

- Enable EFM OAM debugging for received/sent packets tracing.

```
admin@PICOS# set protocols ethernet-oam traceoptions flag packets disable false
admin@PICOS# commit
```

set protocols ethernet-oam traceoptions flag config

The **set protocols ethernet-oam traceoptions flag config** command can be used to enable or disable EFM OAM debugging for configuration tracing.

The **delete protocols ethernet-oam traceoptions flag config** command deletes the configuration.

Command Syntax

set protocols ethernet-oam traceoptions flag config disable <**true | false**>

delete protocols ethernet-oam traceoptions flag config

Parameter

Parameter	Description
<**true	false**>	Enable or disable EFM OAM debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable EFM OAM debugging for configuration tracing. • **false**: Enable EFM OAM debugging for configuration tracing. By default, EFM OAM debugging for configuration tracing is disabled.

Example

- Enable EFM OAM debugging for configuration tracing.

```
admin@PICOS# set protocols ethernet-oam traceoptions flag config disable false
admin@PICOS# commit
```

run show ethernet-oam

The **run show ethernet-oam** command is used to view EFM OAM information and session status.

Command Syntax

run show ethernet-oam [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled EFM OAM. The value is a physical interface. If not specified, EFM OAM information and session status of all the interfaces enabled EFM OAM will be displayed.

Example

- View EFM OAM information and session status.

```
admin@PICOS# run show ethernet-oam interface ge-1/1/1
-------------------------------------------------
Interface ge-1/1/1
Local client
    Admin state:       enable
    OAM Mode:          passive
    OAM timeout:       30 seconds
    Loopback timeout:  3 seconds
    Loopback status:   local loopback
    PDU revision:      3
    OAM status:        SEND_ANY
    PDU:               ANY
Remote client
    MAC address:       18:5a:58:5c:8c:21
    OUI:               48:6e:73
    PDU revision:       3
    OAM Mode:          active
    Unidirection:      not supported
    Link monitor:      not supported
    Remote loopback:   not supported
    MIB retrieval:     not supported
Mtu size:          1500
```

The following table provides the description of the EFM OAM status information in the **run show ethernet-oam command** output.

Item	Description

Admin state	Whether the OAM function of an interface is enabled.
Loopback status	Indicates the status of remote loopback. The value could be **no loopback**, **remote loopback** or **local loopback**. • no loopback: Indicates that a remote loopback has not been established yet. • remote loopback: Indicates that a remote loopback has been established, and the device is the controlling end of the remote loopback, which starts EFM OAM remote loopback tests. • local loopback: Indicates that a remote loopback has been established, and the device is the controlled end of the remote loopback, which responds to the loopback control OAMPDUs from peers.
OAM status	Indicates the OAM status of an interface. The values are as follows: • PASSIVE_WAIT: indicates that the interface is waiting for protocol packets from the peer interface. • ACTIVE_SEND_LOCAL: indicates that the interface is sending protocol packets but fails to negotiate the link status with the peer interface. • ACTIVE_SEND_REMOTE_OK: indicates that the peer interface supports OAM and the negotiation with the peer interface is about to succeed. • SEND_ANY: indicates that the interface successfully negotiates the link status with the peer interface. • FAULT: indicates that the interface is abnormal and fails to establish an OAM connection.
PDU	The way in which the local end processes Ethernet OAMPDUs: • RX_INFO: The interface receives only Information OAMPDUs and does not send any Ethernet OAMPDUs. • LF_INFO: The interface sends only Information OAMPDUs without Information TLV triplets and with their link error flag bits being set. • INFO: The interface sends and receives only Information OAMPDUs. • ANY: The interface sends and receives Ethernet OAMPDUs of any type.

run show ethernet-oam statistics

The **run show ethernet-oam statistics** command is used to view the interface statistics information of EFM OAMPDU packets.

Command Syntax

run show ethernet-oam statistics [**interface** <*interface-name*>]

Parameter

Parameter	Description
interface <*interface-name*>	Optional. Specifies an interface name that enabled EFM OAM. The value is a physical interface. If not specified, statistics information of all the interfaces enabled EFM OAM will be displayed.

Example

- View the statistics information of EFM OAMPDU packets.

```
admin@PICOS# run show ethernet-oam statistics interface ge-1/1/1
Packets statistics for interface ge-1/1/1
Packet type                      OAM Tx Count     OAM Rx Count
-------------------------------------------------------------------------------------
OAMInformation                  11365           11372
OAMLoopbackControl              0               1
OAMUnsupported                  0               0
```

Loopback Detection Commands

- set protocols loopback-detection enable
- set protocols loopback-detection interface enable
- set protocols loopback-detection message-interval
- set protocols loopback-detection traceoptions configuration disable
- set protocols loopback-detection traceoptions all disable
- run show loopback-detection
- run clear loopback-detection interface

set protocols loopback-detection enable

The **set protocols loopback-detection enable** command can be used to enable or disable loopback detection function globally.

The **delete protocols loopback-detection enable** command deletes the configuration.

> **NOTE:**
>
> To enable the loopback detection function, users need to enable loopback detection BOTH globally and at the per-interface level. The command **set protocols loopback-detection interface** <*interface-name*> **enable** <**true | false**> can be used to enable loopback detection function on a specific interface.

Command Syntax

set protocols loopback-detection enable <**true | false**>

delete protocols loopback-detection enable

Parameter

Parameter	Description
enable <**true	false**>	Enable or disable loopback detection function globally. The value could be **true** or **false**. • **true**: Enable loopback detection function globally. • **false**: Disable loopback detection function globally. By default, loopback detection function is disabled.

Example

- Enable loopback detection function globally.

```
admin@PICOS# set protocols loopback-detection enable true
admin@PICOS# commit
```

set protocols loopback-detection interface enable

The **set protocols loopback-detection interface enable** command can be used to enable or disable loopback detection function on a specific interface.

The **delete protocols loopback-detection interface enable** command deletes the configuration.

NOTE:

To enable the loopback detection function, users need to enable loopback detection BOTH globally and at the per-interface level. The command **set protocols loopback-detection enable** <**true | false**> can be used to enable loopback detection function globally.

Command Syntax

set protocols loopback-detection interface <*interface-name*> **enable** <**true | false**>

delete protocols loopback-detection interface <*interface-name*> **enable**

Parameter

Parameter	Description
interface <*interface-name*>	Specifies the interface name. The value is a physical interface or an LAG interface.
enable <**true	false**>	Enable or disable loopback detection function on a specific interface. The value could be **true** or **false**. • **true**: Enable loopback detection function on a specific interface. • **false**: Disable loopback detection function on a specific interface. By default, interface-based loopback detection function is disabled. **NOTE**: Loopback detection can be enabled on a physical interface or a LAG interface but cannot be enabled on the member interface of a LAG interface.

Example

- Enable loopback detection function on interface te-1/1/7.

```
admin@PICOS# set protocols loopback-detection enable true
admin@PICOS# set protocols loopback-detection interface te-1/1/7 enable true
admin@PICOS# commit
```

set protocols loopback-detection message-interval

The **set protocols loopback-detection message-interval** command configures the interval between sending loopback detection messages.

The **delete protocols loopback-detection message-interval** command deletes the configuration.

Command Syntax

set protocols loopback-detection message-interval <*message-interval*>

delete protocols loopback-detection message-interval

Parameter

Parameter	Description
message-interval <*message-interval*>	Specifies the interval between sending loopback detection messages. The value is an integer, in second, that ranges from 10 to 60. The default value is 30 seconds.

Example

- Configure the interval between sending loopback detection messages to 15 seconds.

```
admin@PICOS# set protocols loopback-detection message-interval 15
admin@PICOS# commit
```

set protocols loopback-detection traceoptions configuration disable

The **set protocols loopback-detection traceoptions configuration disable** command can be used to enable or disable loopback detection debugging for configuration tracing.

The **delete protocols loopback-detection traceoptions configuration disable** command deletes the configuration.

Command Syntax

set protocols loopback-detection traceoptions configuration disable <**true | false**>

delete protocols loopback-detection traceoptions configuration disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable loopback detection debugging for configuration tracing. The value could be **true** or **false**. • **true**: Disable loopback detection debugging for configuration tracing. • **false**: Enable loopback detection debugging for configuration tracing. By default, loopback detection debugging for configuration tracing is disabled.

Example

- Enable loopback detection debugging for configuration tracing.

```
admin@PICOS# set protocols loopback-detection traceoptions config disable false
admin@PICOS# commit
```

set protocols loopback-detection traceoptions all disable

The **set protocols loopback-detection traceoptions all disable** command can be used to enable or disable loopback detection debugging for tracing all the loopback-detection operations.

The **delete protocols loopback-detection traceoptions all disable** command deletes the configuration.

Command Syntax

set protocols loopback-detection traceoptions all disable <**true | false**>

delete protocols loopback-detection traceoptions all disable

Parameter

Parameter	Description
disable <**true	false**>	Enable or disable loopback detection debugging for tracing all the loopback-detection operations. The value could be **true** or **false**. • **true**: Disable loopback detection debugging for tracing all the loopback-detection operations. • **false**: Enable loopback detection debugging for tracing all the loopback-detection operations. By default, loopback detection debugging for tracing all the loopback-detection operations is disabled.

Example

- Enable loopback detection debugging for tracing all the loopback-detection operations.

```
admin@PICOS# set protocols loopback-detection traceoptions all disable false
admin@PICOS# commit
```

run show loopback-detection

The **run show loopback-detection** command is used to view the configuration information and status information of loopback detection.

Command Syntax

run show loopback-detection

Parameter

None.

Example

- View the configuration information and status information of loopback detection.

```
admin@PICOS# run show loopback-detection
Loopback-detection: enabled
message-interval: 30s

Interface       LBD Tx    Status                From_Port
----------      ----------    ------------          -----------
ge-1/1/1        true          Normal
ge-1/1/2        false         LoopDetected    ge-1/1/1
......
```

Field	Description
Loopback-detection	Indicates whether loopback detection is globally enabled.
message-interval	Indicates the interval between sending loopback detection packets, in seconds.
Interface	All the physical interfaces or LAG interfaces on the device are displayed.
LBD Tx	Indicate whether the interface is the sending interface of the Loopback Detection (LBD) message, the value could be **true** or **false**. • **true**: indicates that the interface is the sending interface of the Loopback Detection (LBD) message. • **false**: indicates that the interface is not the sending interface of the Loopback Detection (LBD) message.
Status	If an interface receives a Loopback Detection (LBD) message sent from this device, then a loopback is detected, the Status of this interface is **LoopDetected**. The Status of other interfaces are **Normal**.
From_Port	When a loopback is detected, this field indicates the sending interface of loopback detection packets.

run clear loopback-detection interface

The **run clear loopback-detection interface** command is used to clear the ***err-disable*** state of the loopback detection interface.

Command Syntax

run clear loopback-detection interface {*<interface-name>* | **all**}

Parameter

Parameter	Description
interface {*<interface-name>* | **all**}	Specifies the interface name. The value is a physical interface or an LAG interface. If **all** is specified, clear the ***err-disable*** state for all the loopback detection interfaces.

Example

- Clear the ***err-disable*** state of the loopback detection interface xe-1/1/1.

```
admin@PICOS# run clear loopback-detection interface xe-1/1/1
Clear xe-1/1/1 err-disable state
```

PICOS Open vSwitch Command Reference . . . 3
ovs－appctl Commands . . . 4
ovs-appctl Common Commands . . . 5
ovs-appctl Help . . . 6
ovs-appctl hwlog/set-level <module> <level> . . . 7
ovs-appctl hwlog/set-type <mode> <type> . . . 8
ovs-appctl ofproto/set_L34_enable . . . 9
ovs-appctl Version . . . 10
ovs-appctl vlog/list . . . 11
ovs-appctl vlog/set . . . 13
Pica8 Commands . . . 14
ovs-appctl Target Commands . . . 18
ovs-appctl -t ovs-vswitchd <command> . . . 19
ovs－ofctl Commands . . . 20
ovs-ofctl Common Commands . . . 23
ovs-ofctl add-flow <bridge> <flow> . . . 24
ovs-ofctl add-flows <bridge> <file> . . . 29
ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions> . . . 30
ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter> . . . 32
ovs-ofctl bundle <bridge> <bundle> . . . 33
ovs-ofctl del-flows <bridge> <flow> . . . 35
ovs-ofctl del-group <bridge> [group_id=<id>] . . . 36
ovs-ofctl del-meter <bridge> meter=<id> . . . 37
ovs-ofctl del-meters <bridge> . . . 38
ovs-ofctl dump-desc <bridge> . . . 39
ovs-ofctl dump-flows <bridge> <flow> . . . 40
ovs-ofctl dump-ports <bridge> <port> . . . 41
ovs-ofctl dump-ports-desc <bridge> . . . 42
ovs-ofctl dump-tables <bridge> . . . 43
ovs-ofctl dump-tables-desc <bridge> . . . 44
ovs-ofctl mod-flows <bridge> <flow> . . . 45
ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions> . . . 46
ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter> . . . 47
ovs-ofctl mod－port <bridge> <iface> <action> . . . 48
ovs-ofctl mod-table <bridge> <table> <mod> . . . 49
ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]] . . . 50
ovs-ofctl show <bridge> . . . 51
ovs-ofctl snoop <bridge> . . . 52
ovs-ofctl replace-flows <bridge> <file> . . . 54
ovs-ofctl diff-flows <source1> <source2> . . . 55
ovs-ofctl add-groups <bridge> <file> . . . 56
ovs-ofctl queue-get-config <bridge> <port> . . . 57
ovs-ofctl meter-stats <bridge> [meter] . . . 58
ovs-ofctl meter-features <bridge> . . . 59
ovs-ofctl dump-meters <bridge> . . . 60

ovs－vsctl Commands 61
Bridge Commands 65
ovs-vsctl add-br 66
ovs-vsctl del-br 67
ovs-vsctl list-br 68
ovs-vsctl set bridge 69
Port Commands 70
ovs-vsctl add-port 72
ovs-vsctl list-ports 73
ovs-vsctl del-port 74
Controller commands 75
Database commands 77
Interface commands 81
Mirror Commands 82
NetFlow Commands 85
Open vSwitch commands 86
Match-mode Command 87
QoS_queue Commands 89
sFlow commands 90
Cos-map Command 91
Egress-mode Command 93
Set-flow-counter-mode Command 94
Combinated-mode Command 96
DSCP Commands 97

PICOS Open vSwitch Command Reference

Pica8 PicOS software leverages Open vSwitch, a production quality, multi-layer virtual switch licensed under the open source Apache 2.0 license. OVS runs as a process within PicOS. The OpenFlow protocol is driven by the Open Networking Foundation (ONF), a leader in software-defined networking (SDN). The OpenFlow protocol governs three essential components of SDN, including an OpenFlow physical switch, an OpenFlow virtual switch to manage virtual machines, and an OpenFlow controller to organize all network pieces.

NOTE: FS S3410 Series Switch Does Not Support OVS Mode.The Following Content Is Not Applicable to FS S3410 Series of Switches.

Organization

This document presents OVS commands arranged in three major sections:

- **ovs−appctl:** Utility for querying and controlling **ovs-vswitchd** (Open vSwitch daemon)
- **ovs-ofctl:** OpenFlow switch management utility
- **ovs-vsctl:** Utility for configuring and controlling **ovs-vswitchd** (Open vSwitch daemon)

Additional Resources

For detailed information about Open vSwitch, OpenFlow, and command usage, visit the following web sites:

- **Open vSwitch Advanced Features Tutorial**
- **Open vSwitch**
- **OpenFlow**

ovs−appctl Commands

- ovs-appctl Common Commands
- ovs-appctl Target Commands

ovs−ofctl Commands

- ovs-ofctl Common Commands
- ovs-ofctl dump-meters <bridge>

ovs−vsctl Commands

- Bridge Commands
- Port Commands
- Controller commands
- Database commands
- Interface commands
- Mirror Commands
- NetFlow Commands
- Open vSwitch commands
- Match-mode Command
- QoS_queue Commands
- sFlow commands
- Cos-map Command
- Egress-mode Command
- Set-flow-counter-mode Command
- Combinated-mode Command
- DSCP Commands

ovs−appctl Commands

ovs−appctl is a utility for querying and controlling the Open vSwitch daemon.

User can view the **ovs-appctl** help for more information about the utility.

```
admin@Leaf1$ovs-appctl --help
ovs-appctl, for querying and controlling Open vSwitch daemon
usage: ovs-appctl [TARGET] COMMAND [ARG...]
Targets:
  -t, --target=TARGET  pidfile or socket to contact
Common commands:
  help               List commands supported by the target
  version            Print version of the target
  vlog/list          List current logging levels
  vlog/set [SPEC]
      Set log levels as detailed in SPEC, which may include:
      A valid module name (all modules, by default)
      'syslog', 'console', 'file' (all facilities, by default))
      'off', 'emer', 'err', 'warn', 'info', or 'dbg' ('dbg', bydefault)
  vlog/reopen        Make the program reopen its log file
Other options:
  --timeout=SECS     wait at most SECS seconds for a response
  -h, --help         Print this helpful information
  -V, --version      Display ovs-appctl version information
```

User may also view the ovs-appctl manual page for detailed syntax and additional information.

```
admin@Leaf1$man ovs-appctl
ovs-appctl(8)                Open vSwitch Manual               ovs-appctl(8)
NAME
       ovs-appctl - utility for configuring running Open vSwitch daemons
SYNOPSIS
       ovs-appctl [--target=target | -t target] command [arg...]
       ovs-appctl --help
       ovs-appctl --version
DESCRIPTION
       Open  vSwitch  daemons  accept  certain  commands at runtime to control
       their behavior and query their settings.  Every daemon accepts a common
       set  of  commands documented under COMMON COMMANDS below.  Some daemons
       support  additional  commands  documented  in  their  own  manpages.
       ovs-vswitchd in particular accepts a number of additional commands doc-
       umented in ovs-vswitchd(8).
       The ovs-appctl program provides a simple way to invoke these  commands.
       The  command  to  be  sent is specified on ovs-appctl's command line as
       non-option arguments.  ovs-appctl sends the command and prints the dae-
       mon's response on standard output.
<Some output omitted>
```

.

- ovs-appctl Common Commands
- ovs-appctl Target Commands

ovs-appctl Common Commands

This section includes the common comands of ovs-appctl.

- ovs-appctl Help
- ovs-appctl hwlog/set-level <module> <level>
- ovs-appctl hwlog/set-type <mode> <type>
- ovs-appctl ofproto/set_L34_enable
- ovs-appctl Version
- ovs-appctl vlog/list
- ovs-appctl vlog/set
- Pica8 Commands

ovs-appctl Help

Lists commands supported by the ovs-vswitchd.

ovs-appctl hwlog/set-level <module> <level>

Set hwlog level of <module> as detailed in <level>.
The <module> contains sdk/api/all; the <level> contains debug/info/warn/error|/off.

ovs-appctl hwlog/set-level all debug

Set hwlog level of 'all' module as 'debug'.

ovs-appctl hwlog/set-level sdk debug

Set hwlog level of 'sdk' module as 'debug'.

ovs-appctl hwlog/set-level api debug

Set hwlog level of 'api' module as 'debug'.

ovs-appctl hwlog/set-type <mode> <type>

Enable/disable hwlog of <mode>.
The <mode> contains config/packet/all; the <type> contains true/false.

ovs-appctl hwlog/set-type config true

Enable hwlog of configurations.

ovs-appctl ofproto/set_L34_enable

To control whether or not flows unsupported by the hardware can be added, use the **ovs-appctl ofproto/set_L34_enable** command in OVS mode.

Command Syntax

ovs-appctl ofproto/set_L34_enable { **true** | **false** }

Parameters

true	Flows not supported by hardware can be added. This is the default option.
false	Flows not supported by hardware cannot be added.

ovs-appctl Version

ovs-appctl version

Print the version of the ovs-vswitchd.

Example

```
admin@PicOS-OVS$ovs-appctl version
ovs-vswitchd (Open vSwitch) 2.3.0
Compiled May 27 2015 23:04:41
```

ovs-appctl vlog/list

To list the known logging modules and their current levels, use the **ovs-appctl vlog/list** command.

Syntax

ovs-appctl vlog/list

Parameters

There are no parameters for this command.

Examples

The following example lists the known logging modules and their current levels:

```
admin@Switch$ovs-appctl vlog/list
                console    syslog    file
                -------    ------    ------
backtrace         INFO       INFO       INFO
bfd               INFO       INFO       INFO
bond              INFO       INFO       INFO
bridge            INFO       INFO       INFO
bundle            INFO       INFO       INFO
bundles           INFO       INFO       INFO
cfm               INFO       INFO       INFO
classifier        INFO       INFO       INFO
collectors        INFO       INFO       INFO
command_line      INFO       INFO       INFO
connmgr           INFO       INFO       INFO
coverage          INFO       INFO       INFO
daemon            INFO       INFO       INFO
daemon_unix       INFO       INFO       INFO
dpif              INFO       INFO       INFO
dpif_linux        INFO       INFO       INFO
dpif_netdev       INFO       INFO       INFO
dpif_pica         INFO       INFO       INFO
entropy           INFO       INFO       INFO
fail_open         INFO       INFO       INFO
fatal_signal      INFO       INFO       INFO
hmap              INFO       INFO       INFO
hwlog             INFO       INFO       INFO
in_band           INFO       INFO       INFO
inband_bridge     INFO       INFO       INFO
ipfix             INFO       INFO       INFO
jsonrpc           INFO       INFO       INFO
lacp              INFO       INFO       INFO
lcmgr             INFO       INFO       INFO
lcmgr_shared      INFO       INFO       INFO
lldp              INFO       INFO       INFO
lockfile          INFO       INFO       INFO
memory            INFO       INFO       INFO
meta_flow         INFO       INFO       INFO
multipath         INFO       INFO       INFO
netdev            INFO       INFO       INFO
netdev_dummy      INFO       INFO       INFO
netdev_linux      INFO       INFO       INFO
netdev_pica       INFO       INFO       INFO
netdev_pica_lag   INFO       INFO       INFO
netdev_pica_vport  INFO       INFO       INFO
netdev_vport      INFO       INFO       INFO
netflow           INFO       INFO       INFO
netlink           INFO       INFO       INFO
```

```
netlink_notifier  INFO       INFO       INFO
netlink_socket    INFO       INFO       INFO
nx_match          INFO       INFO       INFO
odp_util          INFO       INFO       INFO
ofp_actions       INFO       INFO       INFO
ofp_errors        INFO       INFO       INFO
ofp_msgs          INFO       INFO       INFO
ofp_util          INFO       INFO       INFO
ofproto           INFO       INFO       INFO
ofproto_dpif      INFO       INFO       INFO
ofproto_dpif_mirror  INFO       INFO       INFO
ofproto_dpif_monitor  INFO       INFO       INFO
ofproto_dpif_upcall  INFO       INFO       INFO
ofproto_dpif_xlate  INFO       INFO       INFO
ovs_rcu           INFO       INFO       INFO
ovs_thread        INFO       INFO       INFO
ovsdb_error       INFO       INFO       INFO
ovsdb_idl         INFO       INFO       INFO
pcap              INFO       INFO       INFO
pica_private      INFO       INFO       INFO
pktbuf            INFO       INFO       INFO
poll_loop         INFO       INFO       INFO
process           INFO       INFO       INFO
rconn             INFO       INFO       INFO
reconnect         INFO       INFO       INFO
route_table       INFO       INFO       INFO
sflow             INFO       INFO       INFO
signals           INFO       INFO       INFO
socket_util       INFO       INFO       INFO
stp               INFO       INFO       INFO
stream            INFO       INFO       INFO
stream_fd         INFO       INFO       INFO
stream_ssl        INFO       INFO       INFO
stream_tcp        INFO       INFO       INFO
stream_unix       INFO       INFO       INFO
svec              INFO       INFO       INFO
system_stats      INFO       INFO       INFO
timeval           INFO       INFO       INFO
tunnel            INFO       INFO       INFO
unixctl           INFO       INFO       INFO
user_config       INFO       INFO       INFO
util              INFO       INFO       INFO
vconn             INFO       INFO       INFO
vconn_stream      INFO       INFO       INFO
vlandev           INFO       INFO       INFO
vlog              INFO       INFO       INFO
vswitchd          INFO       INFO       INFO
xenserver         INFO       INFO       INFO
```

ovs-appctl vlog/set

To enable Open vSwitch logging and customize the logging levels, use the **ovs-appctl vlog/set** command.

Syntax

ovs-appctl vlog/set *module*[**:***facility*[**:***level*]]

Parameters

Parameters	
module	A valid module name, as displayed by the ovs-appctl vlog/list command. The log level change is only applied to the specified module. If *module* is not specified, the new settings are applied to all modules.
facility	The log level change is limited to the specified facility. Valid options are **syslog**, **console**, and **file**.
level	Messages of the given severity or higher will be logged, and messages of lower severity will be filtered out. Valid options are **off**, **emer**, **err**, **warn**, **info**, or **dbg**. **off** filters out all messages. If *level* is not specified, the logging level is set to **dbg** (debugging).

Examples

The following example configures debugging messages for Open vSwitch daemon to be logged to the console:

```
admin@Switch$ovs-appctl vlog/set vswitchd:console:dbg
```

Pica8 Commands

Command List

ovs-appctl pica/show

This command displays available resources for open flow.

```
Max Hardware Flow Entry Limitation:
    TCAM Table    : 8192
    Egress Table  : 512
    VFilter Table : 512
    L2 Table      : 32768
    L3 Table      : 24000

Valid Interfaces On Switch as5812_54x:
    Physical interfaces:
        te-1/1/1(1)       te-1/1/2(2)       te-1/1/3(3)       te-1/1/4(4)
        te-1/1/5(5)       te-1/1/6(6)       te-1/1/7(7)       te-1/1/8(8)
        te-1/1/9(9)       te-1/1/10(10)     te-1/1/11(11)     te-1/1/12(12)
        te-1/1/13(13)     te-1/1/14(14)     te-1/1/15(15)     te-1/1/16(16)
        te-1/1/17(17)     te-1/1/18(18)     te-1/1/19(19)     te-1/1/20(20)
        te-1/1/21(21)     te-1/1/22(22)     te-1/1/23(23)     te-1/1/24(24)
        te-1/1/25(25)     te-1/1/26(26)     te-1/1/27(27)     te-1/1/28(28)
        te-1/1/29(29)     te-1/1/30(30)     te-1/1/31(31)     te-1/1/32(32)
        te-1/1/33(33)     te-1/1/34(34)     te-1/1/35(35)     te-1/1/36(36)
        te-1/1/37(37)     te-1/1/38(38)     te-1/1/39(39)     te-1/1/40(40)
        te-1/1/41(41)     te-1/1/42(42)     te-1/1/43(43)     te-1/1/44(44)
        te-1/1/45(45)     te-1/1/46(46)     te-1/1/47(47)     te-1/1/48(48)
        xe-1/1/1(73)      xe-1/1/2(74)      xe-1/1/3(75)      xe-1/1/4(76)
        xe-1/1/5(77)      xe-1/1/6(78)
    LAG   interfaces:    ae1(1025) - ae1023(2047)
    Bond  interfaces:  bond1(2049) - bond1023(3071)
    GRE   interfaces:   gre1(3073) - gre1023(4095)
    VXLAN interfaces: vxlan1(4097) - vxlan1023(5119)
    L2GRE interfaces: l2gre1(5121) - l2gre1023(6143)
```

ovs-appctl bridge/clear-counts bridge *[interface]*

This command clears ports statistics.

```
admin@PicOS-OVS$ovs-appctl bridge/clear-counts br0
admin@PicOS-OVS$ovs-appctl bridge/clear-counts br0 ge-1/1/1
```

ovs-appctl pica/dump-flows [--sort | --rsort]

Shows the hardware flow.

User can use [--sort|--rsort]to sort the output of the hardware flow dump by priority.

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#4 normal permanent flow_id=7 priority=2,in_port=49, actions:50
#0 normal_d permanent flow_id=2 priority=0, actions:drop
#5 normal permanent flow_id=8 priority=3,in_port=51, actions:50
Total 3 flows in HW.

admin@PicOS-OVS$ovs-appctl pica/dump-flows --sort
#0 normal_d permanent flow_id=2 priority=0, actions:drop
```

```
#4 normal permanent flow_id=7 priority=2,in_port=49, actions:50
#5 normal permanent flow_id=8 priority=3,in_port=51, actions:50
Total 3 flows in HW.

admin@PicOS-OVS$ovs-appctl pica/dump-flows --rsort
#5 normal permanent flow_id=8 priority=3,in_port=51, actions:50
#4 normal permanent flow_id=7 priority=2,in_port=49, actions:50
#0 normal_d permanent flow_id=2 priority=0, actions:drop
Total 3 flows in HW.
```

ovs-appctl bridge/dump-flows bridge

Shows all software flows, including those flows not added by user or switch.

```
admin@SpineA-OVS$ovs-appctl bridge/dump-flows br0
duration=2402s, n_packets=n/a, n_bytes=0, priority=24600,dl_vlan=4094,dl_dst=02:00:00:08:00:01/ff:03:ff:ff:ff:ff,ac
duration=2402s, n_packets=n/a, n_bytes=0, priority=24600,dl_vlan=4094,dl_dst=02:00:00:08:00:02/ff:03:ff:ff:ff:ff,ac
duration=2656s, n_packets=n/a, n_bytes=0, priority=22016,ip,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,nw
duration=2656s, n_packets=n/a, n_bytes=0, priority=22016,ip,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,nw
duration=2658s, n_packets=n/a, n_bytes=38984, priority=65535,dl_type=0x88cc,actions=CONTROLLER:65535
duration=2656s, n_packets=n/a, n_bytes=0, priority=22000,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,actio
duration=2656s, n_packets=n/a, n_bytes=0, priority=22000,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00,actio
duration=2656s, n_packets=n/a, n_bytes=23628, priority=2,in_port=1,actions=CONTROLLER:65535
duration=2656s, n_packets=n/a, n_bytes=15710, priority=2,in_port=2,actions=CONTROLLER:65535
duration=53s, n_packets=n/a, n_bytes=1152296, priority=25000,in_port=1,dl_vlan=100,dl_src=00:0c:29:fd:75:ae,dl_dst=
duration=48s, n_packets=n/a, n_bytes=1588, priority=25000,in_port=2,dl_vlan=100,dl_src=00:0c:29:70:2e:b8,dl_dst=00:
duration=2658s, n_packets=n/a, n_bytes=0, priority=0,actions=drop
duration=2656s, n_packets=n/a, n_bytes=576, priority=22016,arp,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00
duration=2656s, n_packets=n/a, n_bytes=1220, priority=22016,arp,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:0
duration=2656s, n_packets=n/a, n_bytes=512, priority=22016,rarp,in_port=2,dl_dst=01:00:00:00:00:00/01:00:00:00:00:0
duration=2656s, n_packets=n/a, n_bytes=512, priority=22016,rarp,in_port=1,dl_dst=01:00:00:00:00:00/01:00:00:00:00:0
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=1,actions=drop
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=0,reg0=0x3,actions=drop
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=0,reg0=0x1,actions=controller(reason=no_match)
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=0,reg0=0x2,actions=drop
table_id=254, duration=2658s, n_packets=n/a, n_bytes=0, priority=2,recirc_id=0,actions=resubmit(,0)
```

ovs-appctl cfm/set-fault *[interface]* normal|false|true

If true, a CFM fault was manually triggered.
If false, force to set no CFM fault.
If normal, return to normal CFM.

ovs-appctl cfm/show *[interface]*

Show cfm status.

```
admin@PicOS-OVS$ovs-appctl cfm/show
---- te-1/1/49 ----
MPID 2000: extended fault_override
fault: override
average health: 100
opstate: up
remote_opstate: up
interval: 1000ms
next CCM tx: 879ms
next fault check: 165ms
Remote MPID 2100
recv since check: true
opstate: up
---- te-1/1/50 ----
MPID 2001: extended fault_override
fault: override
average health: 100
opstate: up
remote_opstate: up
interval: 1000ms
next CCM tx: 879ms
next fault check: 569ms
```

```
Remote MPID 2101
recv since check: true
opstate: up
```

ovs-appctl inband/dump-flows bridge

Show inband flows.

ovs-appctl inband/enable true|false

Enable or disable inband mode.

ovs-appctl inband/show

Show inband status.

ovs-appctl lacp/show

This command displays the LACP status on the configured ports.

```
admin@PicOS-OVS$ovs-appctl lacp/show
---- ae1 ----

status: active negotiated
sys_id:00:11:11:11:11:11
sys_priority: 32768
aggregation key: 1
lacp_time: fast

slave: ge-1/1/1:
current attached
port_id: 1
port_priority: 32768
may_enable: true
actor sys_id:00:11:11:11:11:11
actor sys_priority:32768
actor port_id: 1
actor port_priority:32768
actor key: 1
actor state: activity timeout synchronized collecting distributing
partner sys_id:00:0c:29:fd:75:b8
partner sys_priority: 65535
partner port_id: 2
partner port_priority:255
partner key: 17
partner state: activity timeout aggregation synchronized collecting distributing
---- ae2 ----
status: passive
sys_id: ff:ff:ff:ff:ff:00
sys_priority: 32768
aggregation key: 3
lacp_time: slow

slave: te-1/1/3: current detached
port_id: 3
port_priority: 32768
may_enable: false

actor sys_id: ff:ff:ff:ff:ff:00
actor sys_priority: 32768
actor port_id: 3
actor port_priority: 32768
actor key: 3
actor state: collecting distributing

partner sys_id: ff:ff:ff:ff:ff:00
partner sys_priority: 32768
partner port_id: 2
partner port_priority: 32768
```

```
partner key: 2
partner state: activity collecting distributing
```

ovs-appctl Target Commands

This section includes one command of target. ovs-appctl -t <target> <command> The default <target> is ovs-vswitchd.

- ovs-appctl -t ovs-vswitchd <command>

ovs-appctl -t ovs-vswitchd <command>

ovs-appctl -t ovs-vswitchd lacp/show

Display the information of LACP.

ovs-appctl -t ovs-vswitchd dpif/dump-flows <bridge>

This command can be used in OVS 2.0.

ovs-appctl -t ovs-vswitchd bridge/dump-flows <bridge>

ovs-appctl -t ovs-vswitchd pica/dump-flows

This command can be used in OVS 2.0. Using this command user can print hardware flows..

ovs−ofctl Commands

ovs−ofctl is a utility for managing OpenFlow switches. **ovs-ofctl** should work with any OpenFlow switch, not just Open vSwitch.

Users can view the **ovs-ofctl** help for more information about the utility.

```
admin@Leaf1$ovs-ofctl --help
ovs-ofctl: OpenFlow switch management utility
usage: ovs-ofctl [OPTIONS] COMMAND [ARG...]
For OpenFlow switches:
  show SWITCH                 show OpenFlow information
  dump-desc SWITCH            print switch description
  dump-tables SWITCH          print table stats
  dump-table-features SWITCH  print table features
  mod-port SWITCH IFACE ACT   modify port behavior
  mod-table SWITCH MOD        modify flow table behavior
  get-frags SWITCH            print fragment handling behavior
  set-frags SWITCH FRAG_MODE  set fragment handling behavior
  dump-ports SWITCH [PORT]    print port statistics
  dump-ports-desc SWITCH [PORT]  print port descriptions
  dump-flows SWITCH           print all flow entries
  dump-flows SWITCH FLOW      print matching FLOWs
  dump-aggregate SWITCH       print aggregate flow statistics
  dump-aggregate SWITCH FLOW  print aggregate stats for FLOWs
  queue-stats SWITCH [PORT [QUEUE]]  dump queue stats
  add-flow SWITCH FLOW        add flow described by FLOW
  add-flows SWITCH FILE       add flows from FILE
  mod-flows SWITCH FLOW       modify actions of matching FLOWs
  del-flows SWITCH [FLOW]     delete matching FLOWs
  replace-flows SWITCH FILE   replace flows with those in FILE
  diff-flows SOURCE1 SOURCE2  compare flows from two sources
  packet-out SWITCH IN_PORT ACTIONS PACKET...
                              execute ACTIONS on PACKET
  monitor SWITCH [MISSLEN] [invalid_ttl] [watch:[...]]
                              print packets received from SWITCH
  snoop SWITCH                snoop on SWITCH and its controller
  add-group SWITCH GROUP      add group described by GROUP
  add-groups SWITCH FILE       add group from FILE
  mod-group SWITCH GROUP      modify specific group
  del-groups SWITCH [GROUP]   delete matching GROUPs
  dump-group-features SWITCH  print group features
  dump-groups SWITCH [GROUP]  print group description
  dump-group-stats SWITCH [GROUP]  print group statistics
  queue-get-config SWITCH PORT  print queue information for port
  add-meter SWITCH METER      add meter described by METER
  mod-meter SWITCH METER      modify specific METER
  del-meter SWITCH METER      delete METER
  del-meters SWITCH           delete all meters
  dump-meter SWITCH METER     print METER configuration
  dump-meters SWITCH          print all meter configuration
  meter-stats SWITCH [METER]  print meter statistics
  meter-features SWITCH       print meter features
For OpenFlow switches and controllers:
  probe TARGET                probe whether TARGET is up
  ping TARGET [N]             latency of N-byte echos
  benchmark TARGET N COUNT    bandwidth of COUNT N-byte echos
SWITCH or TARGET is an active OpenFlow connection method.
Other commands:
  ofp-parse FILE              print messages read from FILE
  mod-temp-thresh SWITCH THRESHOLD  modify temperature threshold
  dump-temp-thresh SWITCH     print temperature threshold
  ofp-parse-pcap PCAP         print OpenFlow read from PCAP
  dump-tables-desc SWITCH     print tables description
  bundle SWITCH MSG           send bundle messages
```

```
Active OpenFlow connection methods:
  tcp:IP[:PORT]           PORT (default: 6633) at remote IP
  ssl:IP[:PORT]           SSL PORT (default: 6633) at remote IP
  unix:FILE               Unix domain socket named FILE
PKI configuration (required to use SSL):
  -p, --private-key=FILE  file with private key
  -c, --certificate=FILE  file with certificate for private key
  -C, --ca-cert=FILE      file with peer CA certificate
Daemon options:
  --detach                run in background as daemon
  --no-chdir              do not chdir to '/'
  --pidfile[=FILE]        create pidfile (default: /ovs/var/run/openvswitch/ovs-ofctl.pid)
  --overwrite-pidfile     with --pidfile, start even if already running
OpenFlow version options:
  -V, --version           display version information
  -O, --protocols         set allowed OpenFlow versions
                          (default: OpenFlow10, OpenFlow11, OpenFlow12, OpenFlow13, OpenFlow14)
Logging options:
  -vSPEC, --verbose=SPEC   set logging levels
  -v, --verbose            set maximum verbosity level
  --log-file[=FILE]        enable logging to specified FILE
                           (default: /ovs/var/log/openvswitch/ovs-ofctl.log)
  --syslog-target=HOST:PORT  also send syslog msgs to HOST:PORT via UDP
Other options:
  --strict                   use strict match for flow commands
  --readd                    replace flows that haven't changed
  -F, --flow-format=FORMAT    force particular flow format
  -P, --packet-in-format=FRMT force particular packet in format
  -m, --more                 be more verbose printing OpenFlow
  --timestamp                (monitor, snoop) print timestamps
  -t, --timeout=SECS         give up after SECS seconds
  --sort[=field]             sort in ascending order
  --rsort[=field]            sort in descending order
  --unixctl=SOCKET           set control socket name
  -h, --help                 display this help message
  -V, --version              display version information
```

See ovs-ofctl manual page for detailed syntax and additional information.

```
admin@Leaf1$man ovs-ofctl
ovs-ofctl(8)                                  Open vSwitch Manual                                  ovs-of
NAME
       ovs-ofctl - administer OpenFlow switches
SYNOPSIS
       ovs-ofctl [options] command [switch] [args...]
DESCRIPTION
       The ovs-ofctl program is a command line tool for monitoring and administering OpenFlow switches.  It can als
       the current state of an OpenFlow switch, including features, configuration, and table  entries.   It  should
       with any OpenFlow switch, not just Open vSwitch.
   OpenFlow Switch Management Commands
       These commands allow ovs-ofctl to monitor and administer an OpenFlow switch.  It is able to show the current
       of a switch, including features, configuration, and table entries
<Some output omitted>
```

ovs-ofctl Common Commands

- ovs-ofctl mod-flows <bridge> <flow>
- ovs-ofctl del-group <bridge> [group_id=<id>]
- ovs-ofctl dump-ports <bridge> <port>
- ovs-ofctl mod-table <bridge> <table> <mod>
- ovs-ofctl bundle <bridge> <bundle>
- ovs-ofctl dump-tables-desc <bridge>
- ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl show <bridge>
- ovs-ofctl del-flows <bridge> <flow>
- ovs-ofctl snoop <bridge>
- ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]]
- ovs-ofctl dump-desc <bridge>
- ovs-ofctl dump-ports-desc <bridge>
- ovs-ofctl dump-flows <bridge> <flow>
- ovs-ofctl mod−port <bridge> <iface> <action>

- ovs-ofctl add-flows <bridge> <file>
- ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl del-meters <bridge>
- ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl add-flow <bridge> <flow>
- ovs-ofctl dump-tables <bridge>
- ovs-ofctl del-meter <bridge> meter=<id>
- ovs-ofctl replace-flows <bridge> <file>
- ovs-ofctl diff-flows <source1> <source2>
- ovs-ofctl add-groups <bridge> <file>
- ovs-ofctl queue-get-config <bridge> <port>
- ovs-ofctl meter-stats <bridge> [meter]
- ovs-ofctl meter-features <bridge>

ovs-ofctl dump-meters <bridge>

---

ovs-ofctl Common Commands

Most of these commands take an argument that specifies the method for connecting to an OpenFlow switch. The following connection methods are supported:

- ovs-ofctl add-flow <bridge> <flow>
- ovs-ofctl add-flows <bridge> <file>
- ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl bundle <bridge> <bundle>
- ovs-ofctl del-flows <bridge> <flow>
- ovs-ofctl del-group <bridge> [group_id=<id>]
- ovs-ofctl del-meter <bridge> meter=<id>
- ovs-ofctl del-meters <bridge>
- ovs-ofctl dump-desc <bridge>
- ovs-ofctl dump-flows <bridge> <flow>
- ovs-ofctl dump-ports <bridge> <port>
- ovs-ofctl dump-ports-desc <bridge>
- ovs-ofctl dump-tables <bridge>
- ovs-ofctl dump-tables-desc <bridge>
- ovs-ofctl mod-flows <bridge> <flow>
- ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions>
- ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter>
- ovs-ofctl mod-table <bridge> <table> <mod>
- ovs-ofctl mod−port <bridge> <iface> <action>
- ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]]
- ovs-ofctl show <bridge>
- ovs-ofctl snoop <bridge>
- ovs-ofctl replace-flows <bridge> <file>
- ovs-ofctl diff-flows <source1> <source2>
- ovs-ofctl add-groups <bridge> <file>
- ovs-ofctl queue-get-config <bridge> <port>
- ovs-ofctl meter-stats <bridge> [meter]
- ovs-ofctl meter-features <bridge>

ovs-ofctl add-flow <bridge> <flow>

Add flow described by flow.

ovs-ofctl add-flow <bridge> in_port=<port>,actions=<action>

Matches the in_port port in open flow, <port> can be a port number or keyword (eg:LOCAL).

ovs-ofctl add-flow <bridge> dl_vlan=<vlanid>,actions=<action>

Add a flow with the match field dl_vlan (IEEE 802.1q Virtual LAN tag). When the VLAN ID of the packets matches the flow match field then it will be forward according to the actions.The VLAN value ranges from 0 to 4095.

ovs-ofctl add-flow <bridge> dl_vlan_pcp=<value>,actions=<action>

dl_vlan_pcp is an identifier that matches IEEE 802.1q Priority Code Point (PCP) priority. It is a value between 0 and 7. When the value is higher, frame priority level is higher.

ovs-ofctl add-flow <bridge> dl_src=<mac>,actions=<action>

Add a flow with the match field dl_src that matches an Ethernet source address. This value uses 6 pairs of hexadecimal digits to specify, eg: 00:0B:C4:A8:22:B0.

ovs-ofctl add-flow <bridge> dl_dst=<mac>,actions=<action>

Add a flow with the match field dl_dst that matches an Ethernet destination address. This value uses 6 pairs of hexadecimal digits to specify, eg: 00:0B:C4:A8:22:B0.

ovs-ofctl add-flow <bridge> dl_src=<mac/mask>,actions=<action>

ovs-ofctl add-flow <bridge> dl_dst=<mac/mask>,actions=<action>

This type of source mac address provides a wider match field. When the 6 pairs of masks are full *ff*, it indicates exact match, as to say, it is the same with *dl_src=xx:xx:xx:xx:xx:xx*. Otherwise,1-bit in mask indicates that the corresponding bit in *mac* must match exactly, 0-bit in mask indicates wildcards.

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,actions=<action>

Matches Ethernet protocol type *ethertype*, which is specified as an integer between 0 and 65535, inclusive, either in decimal or as a hexadecimal number prefixed by **0x.** (e.g. **0x0806** to match ARP packet).

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_src=ip[/netmask],actions=<action>

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_dst=ip[/netmask],actions=<action>

nw_src and nw_dst are the identifiers of IP source/destination addresses. But before the IP source/destination address is set, Ethernet Type(dl_type) must be set.Type values include：0x0800: matches IPv4 source/destination address IP (eg:ip, tcp). 0x0806: the arp protocol type, matches the ar_sqa or ar_tpa field. respectively, in ARP packets for IPv4 and Ethernet. 0x8035:therarp protocol type, matches the ar_spa or ar_tpa field, respectively, in RARP packets for IPv4 and Ethernet. Other than 0x0800, 0x0806, or 0x8035, the values of nw_src and nw_dst are ignored

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>, nw_proto=<proto>, actions=<action>

This parameter <proto> is specified as a decimal number with the value between 0-255.
When dl_type=0x86dd or IPv6 is specified, the packets must match IPv6 header type.Set proto to 58 to match ICMPv6 packets.
When dl_type=0x0806 or arp is specified,packets must match the lower 8 bits of the ARP opcodes. The opcodes greater than 255 are treated as 0.
When dl_type=0x8035 or rarp is specified,packets must match the lower 8 bits of the RARP opcodes The opcodes greater than 255 are treated as 0.

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>, nw_tos=<tos>, actions=<action>

This parameter <tos> is specified as a decimal number with the value between 0-255. When dl_type=0x0800 or 0x86dd is specified,matches the IP TOS/DHCP or IPv6 traffic class field tos. Note that the two lower reserved bits of tos are ignored for matching purposes. When **dl_type** is wildcarded or set to a value other than 0x0800 or 0x86dd, the value of **nw_tos** is ignored (see **Flow Syntax** above).

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>, nw_ecn=<ecn>,actions=<action>

This parameter <tos> is specified as a decimal number with the value between 0-3. When dl_type=0x0800 or 0x86dd is specified,matches the *ecn* bits in IP ToS or IPv6 traffic class fields .When **dl_type** is wildcarded or set to a value other than 0x0800 or 0x86dd, the value of **nw_ecn** is ignored

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_proto=<proto>,tp_src=<port>,actions=<action>

ovs-ofctl add-flow <bridge> dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port>,actions=<action>

When you want to match **tp_src** or **tp_dst**, you must specify**dl_type** and **nw_proto**as TCP or UDP , <port> is specified as decimal number between 0-65535. When **dl_type** and **nw_proto** take other values, the values of these settings are ignored.

ovs-ofctl add-flow <bridge> dl_type=<ethernettype>,nw_proto=<proto>,tp_src=<port/mask>,actions=<action>

ovs-ofctl add-flow<bridge> dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port/mask>,actions=<action>

When you set the **tp_src** and **tp_dst** like this, that means bitwise match on TCP (or UDP) source or destination port. Both the port and mask are 16-bit decimal numbers or hexadecimal numbers prefixed by 0X. Each 1bit in mask requires the corresponding bit in port must match, while each 0-bit in mask requires the corresponding bit in port to be ignored.

ovs-ofctl add-flow <bridge> table=<number><flow>

By default, the table number is 0. When **table** number is specified, that will limit flow manipulations and dump flow commands to apply to the specified table number which is between 0-254.

ovs-ofctl add-flow <bridge> metadata=value[/mask]<flow>

metadata is just useful across multiple flow tables. It makes matching flows easy. Sometimes, we will just check the **metadata** of flow because different metadata means different flows. But this field is only applied to software flow tables, not applied to the only hardware flow table in our switch.

ovs-ofctl add-flow<bridge> dl_type=<ethernettype>,nw_proto=1,icmp_type=<type>,actions=<action>

ovs-ofctl add-flow<bridge> dl_type=<ethernettype>,nw_proto=1,icmp_code=<type>,actions=<action>

When you specify **dl_type** and**nw_proto** as ICMP or ICMPv6,then **icmp_type** must matches the ICMP type (eg:**icmp_type=1**), and **icmp_code** must matched ICMP code that the value of code is between 0-255.
When **dl_type** and **nw_proto** take other values, the values of these settings are ignored.

ovs-ofctl add-flow<bridge> dl_type=0x8847,mpls_label=<label>,actions=<action>

The value of mpls label is between 0-1048575.That is to say you can add 1048575 mpls labels at most.

ovs-ofctl add-flow<bridge> dl_type=0x8847,mpls_tc=<tc>,actions=<action>

The value of **mpls_tc** is between 0-7.It is for experimental use.

ovs-ofctl add-flow<bridge> vlan_tci=<tci[/mask]>,actions=<action>

The tci matches VLAN TCI. The tci and mask are 16-bit values are decimal by default;you can use a 0x prefix to set the values in hexadecimal.when mask is specified,1-bit number in mask requires corresponding bit in tci must match exact,and 0-bit in mask makes corresponding bit in tci be ignored.If do not specify mask,thentci is the exact VLAN TCI to match.

ovs-ofctl add-flow<bridge> dl_type=0x86DD,ipv6_src=<ipv6[/netmask]>,actions=<action>

ovs-ofctl add-flow<bridge> dl_type=0x86DD,ipv6_dst=<ipv6[/netmask]>,actions=<action>

If you want to add a flow with the ipv6 source and destination,you must first set the dl_type as 0x86dd(or ipv6 or tcp6).
The actions of flow include the following values,all the values are applied into add-flow, add-flows, and mod-flows .These are just examples of add-flow below.

ovs-ofctl add-flow<bridge><match-field>actions=[target][,target...]

ovs-ofctl add-flow<bridge><match-field>actions=output:<port>

The port should be an OpenFlow port number or keyword as LOCAL and so on.That means outputting packets to port.

ovs-ofctl add-flow<bridge><match-field>actions=enqueue:<port>:<queue>

The *port* should be an OpenFlow port number or keyword(eg:LOCAL).This action means to enqueue the packets on specified *queue* within the port.The queues numbers depend on switch.

ovs-ofctl add-flow<bridge><match-field>actions=NORMAL

This action means making packets be processed as device' normal L2/L3.

ovs-ofctl add-flow<bridge><match-field>actions=flood

This action means outputting packets on all physical ports other than the port on which it was receivedand any ports on which flooding is disabled (typically, these would be ports disabled by the IEEE 802.1D spanning tree protocol).

ovs-ofctl add-flow <bridge> <match-field> actions=all

This action means outputting packets on all physical ports other than the port on which it was received.

ovs-ofctl add-flow <bridge> <match-field>actions=controller(key=value...)

When you set action as controller, the packets will be sent in OpenFlow controller as packet-in message.

ovs-ofctl add-flow <bridge> <match-field>actions=drop

This action means discard the packets without further processing or forwarding. When this action **drop** is used,you should not specify other actions.

ovs-ofctl add-flow <bridge> <match-field> actions=push_vlan:<ethertype>,set_field:<value>-\>vlan_vid,output:<port>

Using **push_vlan**, you can push a new VLAN to packets, *ethertype* is the ethertype for the tag **(**only support **0x8100** at the moment. **set_field** is used to set the value of priority.

ovs-ofctl add-flow <bridge> <match-field> dl_type=<ethertype>,dl_src=<src>,dl_dst=<dst>,actions=push_mpls:<ethertype>,set_field:<value>-\>mpls_label,output:<port>

Using **push_mpls,** you can push a new mpls label for a packet without any mpls label. At this time,the *ethertype* must be either MPLS unicast ethertype**0x8847,** or the MPLS multicast ethertype**0x8848.** if the packets has already contains a mpls label, pushes a new outermost label as a copy of the existing outermost label.

ovs-ofctl add-flow<bridge><match-field>actions=pop_mpls:<ethertype>

You can pop outer mpls label by setting *ethertype*to MPLS Ethertype.and pop all MPLS label by setting *ethertype* to the types except mplsethertype.

ovs-ofctl add-flow<bridge><match-field>actions=push_pbb:<ethertype>,set_field:<value>-\...

You can push outermost mac address for packets.PBB is a mac-in-mac technology.ethertype is **0x88e7.**

ovs-ofctl add-flow<bridge><match-field>actions=pop_pbb

You can pop the outer mac for packets by using pop_pbb.

ovs-ofctl add-flow<bridge><match-field>actions=mod_vlan_vid:<vlan_vid>

This action means modify the thevlan id of the packets.Thevlan tag is added or modified as necessary to match specifiedvalue.when the vlan tag is added ,then priority of the packets are 0 by default.You can set priority by **mod_vlan_pcp**.*vlan_id* is between 0-4095.

ovs-ofctl add-flow<bridge><match-field>actions=mod_vlan_pcp:<vlan_pcp>

You can modify the vlan priority of the packets.vlan_pcp value is between0-7, 0 presents the lowest priority and 7 means highest priority.

ovs-ofctl add-flow<bridge><match-field>actions=strip_vlan

Using this action ,you can pop vlan tag from packets.

ovs-ofctl add-flow<bridge><match-field>actions=mod_dl_src:<mac>

User can modify source mac of packets from the output port by **mod_dl_src.**

ovs-ofctl add-flow<bridge><match-field>actions=mod_dl_dst:<mac>

User can modify *destination* mac of packets from the output port by **mod_dl_dst**

ovs-ofctl add-flow<bridge><match-field>actions=mod_nw_src:<ip>

Modify the *source ipv4* addressof specified flow,by using mod_nw_src.

ovs-ofctl add-flow<bridge><match-field>actions=mod_nw_dst:<ip>

Modify the *destination ipv4* addressof specified flow,by using mod_nw_dst.

ovs-ofctl add-flow<bridge><match-field>actions=mod_tp_src:<port>

Modify the TCP or UDP source port.

ovs-ofctl add-flow<bridge><match-field>actions=mod_tp_dst:<port>

Modify the TCP or UDP destination port.

ovs-ofctl add-flow<bridge><match-field>actions=mod_nw_tos:<tos>

By using this action you can modify the IPv4 TOS or DSCP field to tos, which must be a multiple of 4 between 0-255.This action can not modify the lower 2-bits of tos field which represents ECN bits.

ovs-ofctl add-flow<bridge><match-field>actions=resubmit([port],[table])

By this action,you can re-search OpenFlow flow table with the**in_port** field replaced by *port*. Or research the table whose number is specified by table.

ovs-ofctl add-flow<bridge><match-field>actions=set_queue:<queue>

By taking this action, the packets that is output the port will be output the specified *queue*. Different switch has different numbers of supported queues.

ovs-ofctl add-flow<bridge><match-field>actions=set_mpls_ttl:ttl

This action will set the TTL of outer MPLS label stack entry of a packet. The range of TTL number is between 0-255.

ovs-ofctl add-flow<bridge><match-field>actions=controller(key=value...)

Taking this action will send packets to OpenFlow controller as "packet-in" message. There are some key-value pairs as follow.
max_len=*nbytes:* limit the maximum length of packets sent to the controller. By default, the entire packet is sent.
reason=*reason*:Specify *reason* as the reason for sending the message in the "packet in" message. The supported reasons are **action** (the default), **no_match**, and **invalid_ttl**.

ovs-ofctl add-flow <bridge> in_port=<port>,ip, actions=set_field:16-\>tos,output:<port>

modify the value of tos in packets.

support vntag and vnid in match fields now.

ovs-ofctl add-flow <bridge> vn_tag=0x33330000/0x3FFF0000,dl_dst=00:11:11:11:11:11,actions=2. For the details,check the link:VN-tag.

ovs-ofctl add-flow <bridge> **udp,tp_dst=5000,tun_id=0x0200000000112233,actions=2**

support the udf fields

ovs-ofctl add-flow <bridge> table=250,in_port=<port>,udf0=0x810003E8/0x0000ffff,actions=2

please check the details through the following link:Configuring udf flow

Summarize Above Flows as a Table

ovs-ofctl add-flow <bridge> <flow>

Add table:

feature	Match fields	actions	example
L2	in_port=<port>	<action>	ovs-ofctl add-flow br0 in_port=1,actions=output:2
	dl_src=<mac>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_src=22:22:22:22:22:22,actions=output:2
	dl_dst=<mac>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_dst=00:0B:C4:A8:22:B0,actions=output:2
	dl_src=<mac/mask>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_src=00:0B:C4:A8:22:B0/ff:ff:ff:ff:ff:ff,actions=output:2
	dl_dst=<mac/mask>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_dst=00:0B:C4:A8:22:B0/ff:ff:ff:ff:ff:ff,actions=output:2
	dl_type=<ethernet type>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,actions=output:2
	<match-field>	mod_dl_src:<mac> /set_field:22:22:22:22:33:33-\>dl_dst	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_dst=22:22:22:22:22:22,actions=mod_dl_src:22:23:33:33:33:33,output:2
	<match-field>	mod_dl_dst:<mac> /set_field:22:22:22:22:44:44-\>dl_src	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,actions=mod_dl_dst:22:23:33:33:33:33,output:2
L3	dl_type=<ethernet type>,nw_src=ip[/netmask]	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_src=1.1.1.0/24,actions=output:2
	dl_type=<ethernet type>,nw_dst=ip[/netmask]	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_dst=1.1.1.0/24,actions=output:2
	dl_type=<Ethernet type>, nw_proto=<proto>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,nw_proto=17,actions=set_field:22:33:33:33:33:33-\>dst,output:2
	dl_type=<ethernet type>, nw_ecn=<ecn>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,nw_ecn=1,actions= output:2
	dl_type=<ethernettype>,nw_proto=<proto>,tp_src=<port>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_src=800,actions= output:2
	dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_dst=800,actions= output:2
	dl_type=<ethernettype>,nw_proto=<proto>,tp_src=<port/mask>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_src= 2002/oxffff,actions= output:2
	dl_type=<ethernet type>,nw_proto=<proto>,tp_dst=<port/mask>	<action>	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1, nw_proto =6, tp_dst=2002/oxffff,actions= output:2
	<match-field>	mod_nw_src:<ip> /set_field:2.2.2.2-\>nw_src	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,actions=mod_nw_src:1.1.1.1,output=2
	<match-field>	mod_nw_dst:<ip> /set_field:3.2.2.3-\>nw_dst	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,actions=mod_nw_src:1.1.1.1,output=2
	<match-field>	tcp: mod_tp_src:<port> /set_field:800-\>tp_src udp: set_field:800-\>udp_src	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,tcp,actions=mod_tp_src:2002,output=2 ovs-ofctl add-flow br0 in_port=1,udp,nw_src=1.1.1.1,actions=set_field:800-\>udp_src,output=2
	<match-field>	tcp: mod_tp_dst:<port> /set_field:900-\>tp_dst udp: set_field:800-\>udp_dst	ovs-ofctl add-flow br0 dl_type=0x0800,in_port=1,tcp,actions=mod_tp_dst:2002,output=2 ovs-ofctl add-flow br0 in_port=1,udp,nw_dst=1.1.1.1,actions=set_field:880-\>udp_dst,output=2
Table	table=<number>	<action>	ovs-ofctl add-flow br0 in_port=1,ip,table=251,dl_dst=22:22:22:22:22:22,actions=push_vlan:0x8100,set_field:1999-\>vlan_vid,output:2
Metadata	metadata=value[/mask]	<action>	
ICMP	dl_type=<ethernettype>,nw_proto=1,icmp_type=<type>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_proto=1,icmp_type=0,nw_dst=96.115.0.0/17,actions=meter:2,all
	dl_type=<ethernettype>,nw_proto=1,icmp_code=<type>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_proto=1,icmp_type=8,icmp_code=100,actions=output:2"
MPLS	dl_type=0x8847,mpls_label=<label>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,mpls_label=222,actions=push_mpls:0x8847,set_field:30-\>mpls_label,output:2
	dl_type=0x8847,mpls_tc=<tc>	set_field:<value> -\>mpls_tc	ovs-ofctl add-flow br0 in_port=1,dl_type=0x8847,dl_dst=22:22:22:22:22:22,dl_vlan=2999,mpls_label=333,mpls_tc=1,actions=set_field:2-\>mpls_tc,output:2
	<match-field> dl_type=<ethertype>,dl_src=<src>,dl_dst=<dst>	push_mpls:<ethertype>,set_field:<value>-\>mpls_label,output:<port>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22, actions=push_mpls:0x8847,set_field:222-\>mpls_label,output:2
	<match-field>	pop_mpls:<ethertype>	ovs-ofctl add-flow br0 in_port=5,dl_type=0x8847,dl_dst=22:22:22:22:22:22,dl_vlan=2999,mpls_label=333,mpls_tc=2,actions=push_mpls:0x8847,set_field:222-\>mpls_label,output:6
	<match-field>	set_mpls_ttl:ttl	ovs-ofctl add-flow br0 in_port=5,dl_type=0x8847,dl_dst=22:22:22:22:22:22,dl_vlan=2999,mpls_label=333,actions=push_mpls:0x8847,set_field:222->mpls_label,set_mpls_ttl:253,output:6
VLAN	vlan_tci=<tci[/mask]>	<action>	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=6
	dl_vlan=<vlanid>	<action>	ovs-ofctl add-flow br0 in_port=5,dl_vlan=2999,actions=6
	dl_vlan_pcp=<value>	<action>	ovs-ofctl add-flow br0 in_port=5,dl_vlan_pcp=2,actions=output:6
	<match-field>	push_vlan:<ethertype>,set_field:<value>-\>vlan_vid,output:<port>	ovs-ofctl add-flow br0 in_port=1,ip,actions=push_vlan:0x8100,set_field:2999-\>vlan_vid,output:2

	<match-field>	mod_vlan_vid:<vlan_vid> /set_field:299-\>vlan_vid	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=mod_vlan_vid:888,output:6
	<match-field>	mod_vlan_pcp:<vlan_pcp> /set_field:3-\>vlan_pcp	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=mod_vlan_pcp:5,output:6
	<match-field>	strip_vlan	ovs-ofctl add-flow br0 in_port=5,vlan_tci=0x3bb7/0xffff,actions=strip_vlan,output:6
IPv6	dl_type=0x86DD,ipv6_src= <ipv6[/netmask]>	set_field:2002::1-\>ipv6_src	ovs-ofctl add-flow br0 in_port=1,dl_type=0x86dd,ipv6_src=2001::1/128,actions= set_field:2002::1-\>ipv6_src,output:2
	dl_type=0x86DD,ipv6_dst= <ipv6[/netmask]>	set_field:2002::1-\>ipv6_dst	ovs-ofctl add-flow br0 in_port=1,dl_type=0x86dd,ipv6_dst=2001::1/128,actions= set_field:2002::1-\>ipv6_dst,output:2
Openflow	<match-field>	actions=[target][,target...]	
	<match-field>	actions=output:<port>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_vlan=2999,actions= output:2
	<match-field>	actions=enqueue(port,queue)	ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=enqueue\(1,7\)
	<match-field>	NORMAL	ovs-ofctl add-flow br0 in_port=1,dl_vlan=2999,actions=NORMAL
	<match-field>	flood	ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=flood
	<match-field>	all	ovs-ofctl add-flow br0 in_port=1,dl_vlan=2999,actions=all,set_field:22:33:33:33:33:33-\>dl_dst,output:2,3
	<match-field>	drop	ovs-ofctl add-flow br0 in_port=1,dl_dst=22:22:22:22:22:22,actions=all
	<match-field>	controller(key=value...)	ovs-ofctl add-flow br0 arp,arp_op=1,actions=CONTROLLER
PBB	<match-field>	push_pbb: <ethertype>,set_field: <value>-\>pbb_isid	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,dl_src=22:11:11:11:11:11,dl_dst=22:22:22:22:22:22,actions=push_pbb:0x88e7,push_vlan:0x8100,set_field:4094-\>vlan_vid,output:2
	<match-field>	pop_pbb	ovs-ofctl add-flow br0 in_port=1,dl_type=0x8100,dl_src=00:00:00:11:11:11,dl_dst=00:00:00:22:22:22,actions=pop_vlan,pop_pbb,output:2
	<match-field>	resubmit([port],[table])	ovs-ofctl add-flow br0 table=0,dl_dst=00:00:00:00:11:11,actions=resubmit\(6,1\) Note: at least one "in_port" or "table" must be specified on resubmit
Qos	<match-field>	mod_nw_tos:<tos> /set_field:16-\>ip_dscp	ovs-ofctl add-flow br0 table=253,dl_type=0x0800,nw_dst=1.1.1.1,actions=mod_nw_tos:16
	<match-field>	set_queue:<queue>	ovs-ofctl add-flow br0 in_port=1,dl_src=22:11:11:11:11:11,actions=set_queue:0,output=3
	dl_type=<ethernet type>, nw_tos=<tos>	<action>	ovs-ofctl add-flow br0 in_port=1,dl_type=0x0800,nw_tos=16,nw_dst=1.1.1.1,actions=mod_nw_tos:32

ovs-ofctl add-flows <bridge> <file>

Add multiple flows from file. You can create a file with many flows in the server, and copy this file to your switch. Then use this command **ovs-ofctl add-flows <bridge> <file>** to add these flows in this file.

Command

ovs-ofctl add-flows <bridge> <file>

Example

There are two flows in file 111.txt. Add these flows in this file as below:

admin@PicOS-OVS$sudo scp sophia.sun@10.10.50.20:/home/sophia.sun/111.txt ./
The authenticity of host '10.10.50.20 (10.10.50.20)' can't be established.
ECDSA key fingerprint is 8f:f3:ca:a1:b9:a9:67:26:e1:54:dc:6a:62:74:d5:f6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.50.20' (ECDSA) to the list of known hosts.
sophia.sun@10.10.50.20's password:
111.txt 100% 54 0.1KB/s 00:00
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ls
111.txt
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl add-flows br0 111.txt
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
cookie=0x0, duration=10.804s, table=0, n_packets=n/a, n_bytes=0, in_port=7 actions=output:8
cookie=0x0, duration=10.800s, table=0, n_packets=n/a, n_bytes=0, in_port=8 actions=output:9

ovs-ofctl add-group <bridge> group_id=<id>,type=<type>,bucket=<actions>

PicOS OVS supports group tables from Openflow 1.2.

ovs-ofctl add-group <*bridge*> group_id=<*id*>,type=all,bucket=<*actions*>*[,bucket=<actions>]*

Add a group that group_id=<id>, type=all in <bridge>. The max buckets number can be created is 10.

Example:
Create a group type=all, include two buckets to modify the src-mac and dst-mac.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=1,type=all,bucket=mod_dl_src=00:00:00:11:11:11,mod_dl_dst=00:00:00
```

ovs-ofctl add-group <*bridge*> group_id=<*id*>,type=indirect,bucket=<*actions*>

Add a group that group_id=<id>, type=indirect in <bridge>.

Example:
Create a group type=indirect, just include one bucket to modify the src-mac and dst-mac.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=2,type=indirect,bucket=mod_dl_src=00:00:00:99:11:11,mod_dl_dst=00:
```

ovs-ofctl add-group <*bridge*> group_id=<*id*>,type=select,bucket=<*actions*>*[,bucket=<actions>]*

Add a group that group_id=<id>, type=select in <bridge>.
PisOS OVS is not support weighting now, user cannot specify the weight, weight=1.
Because OVS forwards packets by TCAM, the traditional ECMP in the routing table can not be used in OVS mode.
We implement a "dummy ECMP" by splitting the matching fields of a flow. By the group that type=select, the system will choose one match field to split in nw_src, nw_dst, dl_src, dl_dst. The nw_src is the highest priority, if it has no special nw_src or if the mask of nw_src is 32, it will choose nw_dst. The last choose dl_src and dl_dst. The premise is the match fields must have mask except 32 nor ff:ff:ff:ff:ff:ff.
Exception to this use, is other flows involved with the select group will be packet-driven flows.
Example:
Create a group type=select, the actions of multi buckets only have output.

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=3,type=select,bucket=bucket=output:1,output:2,bucket=output:3,buck
```

ovs-ofctl add-group <*bridge*> group_id=<*id*>,type=ff,bucket=<*actions*>*[,bucket=<actions>]*

Add a group that group_id=<id>, type=ff, in <bridge>. The ff means fast_failover.
Example:

```
admin@PicOS-OVS$ovs-ofctl add-group br0 group_id=4,type=ff,bucket=watch_port:2,watch_group:2,output:3,watch_port:3,
```

Actions supported table:

Chip	Firebolt3								Triumph2	Trident-II		
Model	3290	3295	3920	3922	3930	as5600_52x	3780	as4600_54t	3297	5101	5401	as6701_32x

Chip	Firebolt3								Triumph2	Trident-II		
output<PORT_ID>	√	√	√	√	√	√	√	√	√	√	√	√
mod_dl_src	√	√	√	√	√	√	√	√	√	√	√	√
mod_dl_dst	√	√	√	√	√	√	√	√	√	√	√	√
mod_vlan_vid	√	√	√	√	√	√	√	√	√	√	√	√
mod_vlan_pcp	√	√	√	√	√	√	√	√	√	√	√	√
mod_nw_tos	√	√	√	√	√	√	√	√	√	√	√	√
push_vlan	√	√	√	√	√	√	√	√	√	√	√	√
pop_vlan	√	√	√	√	√	√	√	√	√	√	√	√
strip_vlan	√	√	√	√	√	√	√	√	√	√	√	√
push_pbb	X	X	√	√	√	√	√	X	√	√	√	√
pop_pbb	X	X	√	√	√	√	√	X	√	√	√	√
set_queue	√	√	√	√	√	√	√	√	√	√	√	√
push_mpls	X	X	√	√	√	√	√	X	√	√	√	√
pop_mpls	X	X	√	√	√	√	√	X	√	√	√	√
mod_nw_src	X	X	X	X	X	X	X	X	X	√	√	√
mod_nw_dst	X	X	X	X	X	X	X	X	X	√	√	√
mod_tp_src	X	X	X	X	X	X	X	X	X	√	√	√
mod_tp_dst	X	X	X	X	X	X	X	X	X	√	√	√

The following actions are not supported.

Different modification for a different bucket

eg.

bucket=mod_dl_src:22:11:11:11:11:11,output:2,bucket=mod_dl_src:22:22:22:22:22:22,output:3

ovs-ofctl add-meter <bridge> meter=<id>,<meter-parameter>

> In PicOS OVS, each meter only support configure one meter band.
>
> The counters of one meter are the same as the flow entry counters which the meter applied.

PicOS OVS supports meters from Openflow 1.3. In different Hardware Models, the maximum count of meters that PicOS OVS supports is different. User can use the command to check the maximum count.

```
admin@PicOS-OVS$ovs-ofctl meter-features br0
OFPST_METER_FEATURES reply (OF1.4) (xid=0x2):
max_meter:2048 max_bands:1 max_color:3
band_types: drop dscp_remark
capabilities: kbps burst stats
```

ovs-ofctl add-meter <*bridge*> meter=<*id*>,kbps*[,burst,stats]*,band=type=drop,rate=<*rate*>*[,burst_size=<size>][,prec_level=<level>]*

Add a meter, the type=drop.

Example:

Without burst size. Limit the rate as 30000kbps.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=30000
```

With burst size. Limit the rate as 30000kbps.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,burst,band=type=drop,rate=30000,burst_size=30000
```

ovs-ofctl add-meter <*bridge*> meter=<*id*>,kbps*[,burst,stats]*,band=type= dscp_remark,rate=<*rate*>,prec_level=<*level*>*[,burst_size=<size>]*

Add a meter, the type=dscp_remark.

Example:

Without burst_size. The prec_level=14.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,band=type=dscp_remark,rate=30000,prec_level=14
```

With burst_size. The prec_level=14.

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=2,kbps,burst,band=type=dscp_remark,rate=30000,prec_level=14,burst_size
```

If one meter applies to multiple flow entries, all the flow entries will share the meter rate.

Example:

```
root@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=30000
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=11,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:11,dl_type=0x0800,a
root@PicOS-OVS$ovs-ofctl add-flow br0 in_port=12,dl_dst=22:00:00:00:00:00,dl_src=22:11:11:11:11:22,dl_type=0x0800,a
```

The result: the total rate in port te-1/1/13 is limit to 30000 kbps.

ovs-ofctl bundle <bridge> <bundle>

PicOS OVS supports bundles from version 2.3.

User can add a bundle with the format as follows:

ovs-ofctl bundle <bridge> "[open:bundle_id=<id>,]add:bundle_id=<id>,message=<message>[,add:bundle_id=<id>,message=<message>...] [,close:bundle_id=<id>],commit:bundle_id=<id>"

Using bundles is to group related state changes on a switch so that all changes are applied together, or that none of them is applied. The second goal is to better synchronize changes across a set of OpenFlow switches. Bundles can be prepared and pre-validated on each switch and applied at the same time.

PicOS OVS supports applying 10 bundles maximum at the same time. And the maximum messages is 100 of each bundle.
Also supports port/flow/group/meter-mods at present.

Flow-mod

message=add-flow <match><,actions>

User can add a flow by bundle.
Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=add-flow in_port=1,dl_src=22:11:11:1
```

messag=mod-flows <match><,actions>

Modify flows by bundle.

message=del-flows <match>

Delete flows by bundle.
Example:

Delete the flows that match the field.

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=del-flows in_port=1,commit:bundle_id
```

Delete all flows in br0.

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=del-flows,commit:bundle_id=1"
```

Group-mod

message=add-group group_id=<id>,type=<type>,bucket=<actions>[,bucket=<actions>]

Add groups by bundle.

Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=add-group group_id=1,type=all,bucket
```

message=mod-group group_id=<id>,type=<type>,bucket=<actions>[,bucket=<actions>]

Modify a group by bundle.

message=del-groups group_id=<id>

Delete groups by bundle.
Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 "open:bundle_id=1,add:bundle_id=1,message=del-groups ,commit:bundle_id=1"
```

Meter-mod

message=add-meter meter=<id> kbps[,burst,stats],band=type=<type>,rate=<rate>[,burst_size=<size>,prec_level=<level>]

Add meter by bundle.

message=mod-meter meter=<id> kbps[,burst,stats],band=type=<type>,rate=<rate>[,burst_size=<size>,prec_level=<level>]

Modify meter by bundle.

message=del-meter meter=<id>

Delete meter that meter=<id>.

Port-mod

message=mod-port <port> <down/up/no-receive/receive/no-forward/forward/no-packet-in/packet-in>

Modify port state, the configure must be one of 'down/up/no-receive/receive/no-forward/forward/no-packet-in/packet-in'.

Example:

```
admin@PicOS-OVS$ovs-ofctl bundle br0 'open:bundle_id=1,add:bundle_id=1,message=mod-port te-1/1/1 no-packet-in,commi
```

Multiple bundles

User can apply multiple bundles at the same time. Each bundle has its own open/add/close/commit/discard.
Example:

```
root@PicOS-OVS$ovs-ofctl bundle br-iris "open:bundle_id=1,open:bundle_id=2,add:bundle_id=1,message=add-flow dl_src=
```

ovs-ofctl del-flows <bridge> <flow>

Delete the flow entries from the flow table of <*bridge*>. If the *[flow]* is omitted, delete all flows in <*bridge*>, otherwise, will delete the matched flows.

ovs-ofctl del-group <bridge> [group_id=<id>]

Delete group in <bridge>. If the group_id is specified, the group that <group_id> in <bridge> will delete, otherwise, all groups in <bridge> will be cleared.
Example:

```
admin@PicOS-OVS$ovs-ofctl del-groups br0 group_id=2
admin@PicOS-OVS$ovs-ofctl del-groups br0
```

ovs-ofctl del-meter <bridge> meter=<id>

Delete the meter that meter=<id> in <bridge>.

ovs-ofctl del-meters <bridge>

Delete all the meters in <bridge>.

ovs-ofctl dump-desc <bridge>

Prints <*bridge*> description, including manufacturer, hardware, software, serial number and dp description.

ovs-ofctl dump-flows <bridge> <flow>

Prints flow.entries of <bridge>. With the *[flow]* specified will only print the matching flow. If the *[flow]* is omitted, all flow entries of the bridge will be printed.

ovs-ofctl dump-ports <bridge> <port>

Prints the port statistics of <*bridge*>. If the port is specified, only the port statistics of the bridge will be printed, otherwise, will print all the ports statistics.

ovs-ofctl dump-ports-desc <bridge>

Prints port statistics. Will show detail information about the interfaces in this bridge, including the state, peer and speed information,etc. The information printed by this command is a subset of command 'ovs-ofctl show ***<bridge>'.***

ovs-ofctl dump-tables <bridge>

Prints <*bridge*> all table stats. Including all 254 tables.

ovs-ofctl dump-tables-desc <bridge>

Prints the descriptions of tables of <bridge>.

ovs-ofctl mod-flows <bridge> <flow>

Modify the actions of matching flows in the <*bridge*>.

ovs-ofctl mod-group <bridge> group_id=<id>,type=<type>,bucket=<actions>

Modify a group if the group entry with the specified group identifier already resides in the group table. If the group identifier does not exist, the group will add in group table successfully.
Example:

```
admin@PicOS-OVS$ovs-ofctl mod-group br0 group_id=100,type=indirect,bucket=mod_dl_src=00:00:00:99:11:11,mod_dl_dst=0
```

ovs-ofctl mod-meter <bridge> meter=<id>,<meter-parameter>

Modify a meter if the meter entry with the specified meter identifier already exists.

The format is shown as follows:

ovs-ofctl mod-meter <bridge> meter=<id>,kbps[,burst,stats],band=type=<type>,rate=<rate>,burst_size=<size>,prec_level=<level>

ovs-ofctl mod−port <bridge> <iface> <action>

Modify behaviors of port *<iface>* in *switch*. *<iface>* can be an OpenFlow port number or name, or the **LOCAL** port name. The *<action>* can be as follows:

ovs-ofctl mod-port <bridge> <iface> up

ovs-ofctl mod-port <bridge> <iface> down

Enable or disable the port link status.

ovs-ofctl mod-port <bridge> <iface> receive

ovs-ofctl mod-port <bridge> <iface> no−receive

Allow or disallow this interface to receive traffic. By default, receiving is allowed.

ovs-ofctl mod-port <bridge> <iface> forward

ovs-ofctl mod-port <bridge> <iface> no−forward

Allow or disallow traffic forwarding on this interface. By default, forwarding is allowed.

ovs-ofctl mod-port <bridge> <iface> flood

ovs-ofctl mod-port <bridge> <iface> no−flood

Controls whether the interface is to flood the received traffic or not. By default, flooding is enabled. Disabling flooding is primarily useful to prevent loops when a spanning tree protocol is not in use.

ovs-ofctl mod-table <bridge> <table> <mod>

ovs-ofctl mod-table <bridge> <table> evict

Enable eviction on <table> of <bridge>. Eviction adds a mechanism enabling the switch to automatically eliminate entries of lower importance to make space for newer entries. This enables smoother degradation of behavior when the table is full.
To enable eviction on all tables, user can set the <table> as 'all'.

ovs-ofctl mod-table <bridge> <table> vacancy:<range>

Configure the vacancy <range> on <table> of <bridge>. The vacancy event adds a mechanism enabling the controller to get an early warning based on a capacity threshold chosen by the controller. This allows the controller to react in advance and avoid getting the table full. If user wants to configure vacancy range on all tables, set the <table> as 'all'.
The syntax of <range> as <low..high>.

ovs-ofctl mod-table <bridge> <table> clear

Clear the eviction or vacancy on <table> of <bridge>. If user wants to clear eviction on all tables, set the <table> as 'all'.

ovs-ofctl monitor <bridge> [MISSLEN] [invalid_ttl] [watch:[...]]

Print packets received from <bridge>.

ovs-ofctl show <bridge>

Show OpenFlow information on <*bridge*>, including OpenFlow features and port descriptions.

ovs-ofctl snoop <bridge>

ovs-ofctl snoop br0

This command snoops the bridge for open flow messages exchanged with the controller. It can be used to debug flow installations, modifications and packet_in and packet_out messages on the bridge. This command executes in a continuous loop. ^C should be used to break the display output.

```
admin@SpineA-OVS$ovs-ofctl snoop br0
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REPLY (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REPLY (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_PACKET_IN (OF1.3) (xid=0x0): cookie=0x0 total_len=1516 in_port=1 (via action) data_len=1516 (unbuffered)
udp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:fd:75:ae,dl_dst=00:0c:29:70:2e:b8,nw_src=100.0.0
OFPT_PACKET_OUT (OF1.3) (xid=0x4c): in_port=CONTROLLER actions=output:2 data_len=1516
udp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:fd:75:ae,dl_dst=00:0c:29:70:2e:b8,nw_src=100.0.0
OFPT_FLOW_MOD (OF1.3) (xid=0x4d): ADD priority=25000,in_port=1,dl_vlan=100,dl_src=00:0c:29:fd:75:ae,dl_dst=00:0c:29
OFPT_BARRIER_REQUEST (OF1.3) (xid=0x4e):
OFPT_BARRIER_REPLY (OF1.3) (xid=0x4e):
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_ECHO_REPLY (OF1.3) (xid=0x0): 0 bytes of payload
OFPT_PACKET_IN (OF1.3) (xid=0x0): cookie=0x0 total_len=64 in_port=2 (via action) data_len=64 (unbuffered)
arp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:70:2e:b8,dl_dst=00:0c:29:fd:75:ae,arp_spa=100.0.
OFPT_PACKET_OUT (OF1.3) (xid=0x4f): in_port=CONTROLLER actions=output:1 data_len=64
arp,metadata=0,in_port=0,dl_vlan=100,dl_vlan_pcp=0,dl_src=00:0c:29:70:2e:b8,dl_dst=00:0c:29:fd:75:ae,arp_spa=100.0.
OFPT_FLOW_MOD (OF1.3) (xid=0x50): ADD priority=25000,in_port=2,dl_vlan=100,dl_src=00:0c:29:70:2e:b8,dl_dst=00:0c:29
OFPT_BARRIER_REQUEST (OF1.3) (xid=0x51):
OFPT_BARRIER_REPLY (OF1.3) (xid=0x51):
OFPT_ECHO_REQUEST (OF1.3) (xid=0x0): 0 bytes of payload
```

In case of error conditions, a hex dump of the erroneous packet is displayed.

```
admin@XorPlus$ovs-ofctl snoop br0



OFPT_PACKET_OUT (OF1.3) (xid=0x375f4): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375f5): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375f6): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375f7): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375f8): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375f9): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375fa): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375fb): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x375fc): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375fd): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
```

```
OFPT_PACKET_OUT (OF1.3) (xid=0x375fe): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x375ff): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPST_PORT request (OF1.3) (xid=0x26): port_no=ANY
OFPST_PORT reply (OF1.3) (xid=0x26): 4 ports
  port  1: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=604176.668s
  port  2: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=604121.342s
  port  3: rx pkts=0, bytes=0, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=604091.091s
  port LOCAL: rx pkts=8, bytes=816, drop=0, errs=0, frame=0, over=0, crc=0
           tx pkts=0, bytes=0, drop=0, errs=0, coll=0
           duration=934668.169s
OFPST_FLOW request (OF1.3) (xid=0x37601):
OFPST_FLOW reply (OF1.3) (xid=0x37601):
 cookie=0x1f00007eaab36a, duration=836.005s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=40000,arp ac
 cookie=0x1f00007eaab36a, duration=836.005s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=5,arp action
 cookie=0x1f00007eaa9ce4, duration=836.006s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=5,ip actions
 cookie=0x1f00007ccd1ab0, duration=836.006s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=40000,dl_typ
 cookie=0x1f00007cced5a6, duration=836.006s, table=0, n_packets=n/a, n_bytes=0, send_flow_rem priority=40000,dl_typ
OFPT_FLOW_MOD (OF1.3) (xid=0x0): ***decode error: OFPBMC_BAD_PREREQ***
OFPT_ERROR (OF1.3) (xid=0x0): OFPBMC_BAD_PREREQ
OFPT_FLOW_MOD (OF1.3) (xid=0x0):
(***truncated to 64 bytes from 88***)
00000000  04 0e 00 58 00 00 00 00-00 1f 00 00 a5 d7 3f 26 |...X..........?&|
00000010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 05 |................|
00000020  ff ff ff ff ff ff ff ff-ff ff ff ff 00 01 00 00 |................|
00000030  00 01 00 10 80 00 19 08-e0 00 00 00 f0 00 00 00 |................|
OFPT_PACKET_OUT (OF1.3) (xid=0x37604): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x37605): in_port=CONTROLLER actions=output:1 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x37606): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x37607): in_port=CONTROLLER actions=output:2 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPT_PACKET_OUT (OF1.3) (xid=0x37608): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=01:23:20:00:00:01,dl_type=0x88cc
OFPT_PACKET_OUT (OF1.3) (xid=0x37609): in_port=CONTROLLER actions=output:3 data_len=81
metadata=0,in_port=0,vlan_tci=0x0000,dl_src=de:ad:be:ef:ba:11,dl_dst=ff:ff:ff:ff:ff:ff,dl_type=0x8942
OFPST_GROUP request (OF1.3) (xid=0x3e6b): group_id=ALL
OFPST_GROUP reply (OF1.3) (xid=0x3e6b):
OFPST_GROUP_DESC request (OF1.3) (xid=0x3e6c): group_id=ALL
OFPST_GROUP_DESC reply (OF1.3) (xid=0x3e6c):
^C2015-09-15T17:36:40Z|00001|fatal_signal|WARN|terminating with signal 2 (Interrupt)
```

ovs-ofctl replace-flows <bridge> <file>

ovs-ofctl replace-flows <bridge> <file>

Using this command, you can replace existing flows in the bridge.

Example:

```
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#13 normal permanent recirc_id=0,in_port=10, actions:8,9
#12 normal_d permanent priority=0,recirc_id=0, actions:drop
Total 2 flows in HW.
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl replace-flows br0 file2.txt
admin@PicOS-OVS$ovs-appctl pica/dump-flows
#14 normal permanent recirc_id=0,in_port=8,dl_dst=22:22:22:22:22:33, actions:10
#15 normal permanent recirc_id=0,in_port=8,dl_dst=22:22:22:22:22:22, actions:9
```

ovs-ofctl diff-flows <source1> <source2>

ovs-ofctl diff-flows <source1> <source2>

Compare flows from two sources, you can also compare flows from a bridge and a source.

Example:

```
admin@PicOS-OVS$ls
file1.txt file2.txt
admin@PicOS-OVS$cat file1.txt
in_port=9,dl_vlan=10,actions=output:8
admin@PicOS-OVS$
admin@PicOS-OVS$cat file2.txt
in_port=8,dl_dst=22:22:22:22:22:22,actions=output:9
in_port=8,dl_dst=22:22:22:22:22:33,actions=output:10
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl diff-flows file2.txt file1.txt
-in_port=8,dl_dst=22:22:22:22:22:22 actions=output:9
-in_port=8,dl_dst=22:22:22:22:22:33 actions=output:10
+in_port=9,dl_vlan=10 actions=output:8
```

ovs-ofctl add-groups <bridge> <file>

ovs-ofctl add-groups <bridge> <file>

Add groups to the switch from a file.

Example:

```
admin@PicOS-OVS$cat group.txt
group_id=1,type=all,bucket=output:8
group_id=2,type=select,bucket=output:9,bucket=output:10
admin@PicOS-OVS$ovs-ofctl add-groups br0 group.txt
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$
admin@PicOS-OVS$ovs-ofctl dump-groups br0
OFPST_GROUP_DESC reply (OF1.4) (xid=0x2):
group_id=1,type=all,bucket=actions=output:8
group_id=2,type=select,bucket=actions=output:9,bucket=actions=output:10
admin@PicOS-OVS$
admin@PicOS-OVS$
```

ovs-ofctl queue-get-config <bridge> <port>

ovs-ofctl queue-get-config <bridge> <port>

Print queue information for specified port.

Example:

```
admin@PicOS-OVS$ovs-ofctl queue-get-config br0 ge-1/1/8
OFPT_QUEUE_GET_CONFIG_REPLY (OF1.4) (xid=0x4): port=8
queue 0: port=8 min_rate:1.2% max_rate:1.2%
queue 7: port=8 min_rate:1.2% max_rate:1.2%
```

ovs-ofctl meter-stats <bridge> [meter]

ovs-ofctl meter-stats <bridge> [meter]

Print meter statistics.

Example:

```
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:100 flow_count:0 packet_in_count:0 byte_in_count:0 duration:346.419s bands:
0: packet_count:0 byte_count:0
```

ovs-ofctl meter-features <bridge>

ovs-ofctl meter-features <bridge>

Print meter features.

Example:

```
admin@PicOS-OVS$ovs-ofctl meter-features br0
OFPST_METER_FEATURES reply (OF1.4) (xid=0x2):
max_meter:100 max_bands:1 max_color:3
band_types: drop dscp_remark
capabilities: kbps burst stats
```

ovs-ofctl dump-meters <bridge>

ovs-ofctl dump-meters <bridge>

Print all meter configurations.

ovs-ofctl dump-meter <bridge> [meter_id]

Print METER configuration of this meter_id.

ovs−vsctl Commands

The command **ovs-vsctl** is a utility for querying and configuring the Open vSwitch. The Open vSwitch configuration is kept in a database managed by the **ovsdb-server** process.The **ovs-vsctl** command connects to **ovsdb-server**, which maintains the Open vSwitch configuration database. Using this connection, **ovs-vsctl** queries and applies changes to the database, based on the supplied commands.

See **ovs-vsctl** help for more information about the utility.

```
admin@PICOS-OVS:~$ ovs-vsctl --help
ovs-vsctl: ovs-vswitchd management utility
usage: ovs-vsctl [OPTIONS] COMMAND [ARG...]

Open vSwitch commands:
  init                        initialize database, if not yet initialized
  show                        print overview of database contents
  emer-reset                  reset configuration to clean state

Bridge commands:
  add-br BRIDGE               create a new bridge named BRIDGE
  add-br BRIDGE PARENT VLAN   create new fake BRIDGE in PARENT on VLAN
  del-br BRIDGE               delete BRIDGE and all of its ports
  list-br                     print the names of all the bridges
  br-exists BRIDGE            exit 2 if BRIDGE does not exist
  br-to-vlan BRIDGE           print the VLAN which BRIDGE is on
  br-to-parent BRIDGE         print the parent of BRIDGE
  br-set-external-id BRIDGE KEY VALUE  set KEY on BRIDGE to VALUE
  br-set-external-id BRIDGE KEY  unset KEY on BRIDGE
  br-get-external-id BRIDGE KEY  print value of KEY on BRIDGE
  br-get-external-id BRIDGE  list key-value pairs on BRIDGE

Port commands (a bond is considered to be a single port):
  list-ports BRIDGE           print the names of all the ports on BRIDGE
  add-port BRIDGE PORT        add network device PORT to BRIDGE
  add-bond BRIDGE PORT IFACE...  add bonded port PORT in BRIDGE from IFACES
  del-port [BRIDGE] PORT      delete PORT (which may be bonded) from BRIDGE
  port-to-br PORT             print name of bridge that contains PORT

Interface commands (a bond consists of multiple interfaces):
  list-ifaces BRIDGE          print the names of all interfaces on BRIDGE
  iface-to-br IFACE           print name of bridge that contains IFACE

Controller commands:
  get-controller BRIDGE      print the controllers for BRIDGE
  del-controller BRIDGE      delete the controllers for BRIDGE
  set-controller BRIDGE TARGET...  set the controllers for BRIDGE
  get-fail-mode BRIDGE       print the fail-mode for BRIDGE
  del-fail-mode BRIDGE       delete the fail-mode for BRIDGE
  set-fail-mode BRIDGE MODE  set the fail-mode for BRIDGE to MODE

Manager commands:
  get-manager                print the managers
  del-manager                delete the managers
  set-manager TARGET...      set the list of managers to TARGET...

SSL commands:
  get-ssl                     print the SSL configuration
  del-ssl                     delete the SSL configuration
  set-ssl PRIV-KEY CERT CA-CERT  set the SSL configuration

Switch commands:
  emer-reset                  reset switch to known good state

Database commands:
  list TBL [REC]              list RECord (or all records) in TBL
```

```
  find TBL CONDITION...       list records satisfying CONDITION in TBL
  get TBL REC COL[:KEY]       print values of COLumns in RECord in TBL
  set TBL REC COL[:KEY]=VALUE set COLumn values in RECord in TBL
  add TBL REC COL [KEY=]VALUE add (KEY=)VALUE to COLumn in RECord in TBL
  remove TBL REC COL [KEY=]VALUE  remove (KEY=)VALUE from COLumn
  clear TBL REC COL           clear values from COLumn in RECord in TBL
  create TBL COL[:KEY]=VALUE  create and initialize new record
  destroy TBL REC             delete RECord from TBL
  wait-until TBL REC [COL[:KEY]=VALUE]  wait until condition is true
Potentially unsafe database commands require --force option.

Options:
  --db=DATABASE               connect to DATABASE
                              (default: unix:/ovs/var/run/openvswitch/db.sock)
  --no-wait                   do not wait for ovs-vswitchd to reconfigure
  --retry                     keep trying to connect to server forever
  -t, --timeout=SECS          wait at most SECS seconds for ovs-vswitchd
  --dry-run                   do not commit changes to database
  --oneline                   print exactly one line of output per command

Pica commands:
  show-running-config                           print current ovsdb config
  show-valid-port [FRONT]                       print all valid ports or one
  set-port-breakout ALL|FRONT TRUE|FALSE        use breakout cable or not
  set-port-name FRONT [1,4]=default|XXX         modify name of sub-port on FRONT
  set-match-mode MODE:OPTIONS=PRIORITY          set match-modes
  show-match-mode                               print current match-modes
  set-gtp-udp-dst-ports PORT...                 set gtp udp ports, PORT is up to 4
  show-gtp-udp-dst-ports                        show gtp udp ports
  set-match-vxlan-vni-enable TRUE|FALSE         enable or disable vxlan vni matching
  show-match-vxlan-vni                          show vxlan vni matching
  set-vxlan-udp-dst-port [1, 65535]             set vxlan udp destination port
  show-vxlan-udp-dst-port                       show vxlan udp destination port
  set-vntag-ethertype [0x6000, 0xffff]          set VN tag ethertype
  show-vntag-ethertype                          show VN tag ethertype
  set-snmp-enable TRUE|FALSE                    enable or disable snmp
  show-snmp                                     show snmp
  set-snmp-trap-targets    IPv4(s)              set snmp trap targets
  show-snmp-trap-targets                        show snmp trap targets
  set-snmp-community-name                       set snmp agent community name
  show-snmp-community-name                      show snmp agent community name
  set-cos-map TRUE|FALSE                        enable or disable cos-mapping
  show-cos-map [IFACE]                          show cos-mapping
  set-vlan-priority-cos-map TRUE|FALSE          enable or disable vlan-priority-cos-mapping
  show-vlan-priority-cos-map                    show vlan-priority-cos-mapping
  set-egress-mode TRUE|FALSE [TABLE]            set egress mode
  show-egress-mode                              show egress-mode
  set-combinated-mode TRUE|FALSE                enable or disable combinated-mode
  show-combinated-mode                          show combinated-mode
  set-l2gre-key-length                          set l2gre key length
  show-l2gre-key-length                         show l2gre key length
  set-proxy-arp TRUE|FALSE SUBNETS              set proxy arp
  show-proxy-arp                                show proxy arp
  set-proxy-icmpv6 TRUE|FALSE SUBNETS           set proxy icmpv6 for NS/NA
  show-proxy-icmpv6                             show proxy icmpv6
  set-l2-mode TRUE|FALSE [TABLE]                set l2 mode
  show-l2-mode                                  show l2 mode
  set-l3-mode TRUE|FALSE [TABLE]                set l3 mode
  show-l3-mode                                  show l3 mode
  set-l2-l3-buffer-mode [0, 5]                  set l2/l3 buffer mode(0-5)
  show-l2-l3-buffer-mode                        show l2/l3 buffer mode
  set-l2-l3-preference TRUE|FALSE               set l2/l3 flow preference
  show-l2-l3-preference                         show l2/l3 flow preference
  set-max-ecmp-ports NUM                        set l3 max ecmp ports to NUM(2~32 and a power of 2)
  show-max-ecmp-ports                           show l3 max ecmp ports
  set-lag-advance-hash-mapping-fields FIELDS    set hash fields of advance hash-mapping
  show-lag-advance-hash-mapping-fields          show hash fields of advance hash-mapping
  set-udf-mode MODE                             set udf mode, MODE's format is udfN(l2|l3,offset=OFS,length=LEN),..
                                                only up to 4 udfs(udf0,udf1,udf2,udf3) are supported
  show-udf-mode                                 show udf mode
```

```
  set-max-resilient-hash-lag-count COUNT       set lag-max-resilient-hash-lag-count.
                                               COUNT is max count of lags which,
                                               can be set to resilient hash,
                                               the valid value of COUNT is
                                               1, 2, 4, 8, 16, 32, 64.
                                               The default value is 1.
  show-max-resilient-hash-lag-count            show lag-max-resilient-hash-lag-count.
  set-macro-udf MODE                           set macro udf mode instead of offset and length, look up show udf f
  show-macro-udf                               show macro udf mode
  show-udf-field                               options for macro udf
  set-egress-mc-queue-dynamic [0,7] TRUE|FALSE set certain queue id multicast dynamic buffer enable
  set-egress-shared-queue-ratio [0,7] [0,100]  set certain queue id shared buffer ratio
  show-egress-shared-queue-ratio               show added queue id shared buffer ratio
  set-loopback-enable TRUE|FALSE               set loopback enable or disable
  set-option-match-vlan-type TRUE|FALSE        enable or disable matching untagged pakcets
  show-option-match-vlan-type                  show vlan format enable or disable
  set-select-group-hash-fields [FIELDS]        set select-group-hash-fields
  show-select-group-hash-fields                show current select-group-hash-fields
  set-flow-handling-mode [MODE]                set flow-handling-mode
  show-flow-handling-mode                      show current flow-handling-mode
  set-rdbgc4 [TYPE]                            set rdbgc4
  show-rdbgc4                                  show current rdbgc4
  set-lag-members-sorted                       set lag members sorted
  show-lag-members-sorted                      show lag members sorted
  set-group-ranges [GROUPS]                    set special groups(lag-select-groups, ecmp-select-groups,
                                               ingress-mirror-groups, egress-mirror-groups) ranges
  show-group-ranges                            show current group ranges
  set-meter-ranges [METERS]                    set special meters(egress-meter) ranges
  show-meter-ranges                            show current meter ranges
  set-l3-ecmp-hash-fields FIELDS               set l3 ecmp hash fields
  show-l3-ecmp-hash-fields                     show l3 ecmp hash fields
  set-l3-egress-keep-fields [FIELDS]           set default keep fields in l3 egress interface
  show-l3-egress-keep-fields                   show default keep fields in l3 egress interface
  disable-extend-group TRUE|FALSE              disable or enable extend group for arp/mpls flows
  show-extend-group                            show extend group config
  set-symmetric-hash [LAG|ECMP] TRUE|FALSE     disable or enable symmetric hash
  show-symmetric-hash                          show symmetric hash config
  set-flow-counter-mode both|bytes|packets     set flow counter mode
  show-flow-counter-mode                       show flow counter mode
  set-ttp-enable TRUE|FALSE                    set ttp module enable or disable
  set-ttp-file FILE                            set ttp file name
  show-ttp                                     show ttp status and file name
  set-counter-interval [10,1000]               set counter interval
  show-counter-interval                        show counter interval
  display-settings                             show the configurations in OVSDB through ovs-vsctl comands

Logging options:
  -vSPEC, --verbose=SPEC   set logging levels
  -v, --verbose            set maximum verbosity level
  --log-file[=FILE]        enable logging to specified FILE
                           (default: /ovs/var/log/openvswitch/ovs-vsctl.log)
  --syslog-target=HOST:PORT  also send syslog msgs to HOST:PORT via UDP
  --no-syslog              equivalent to --verbose=vsctl:syslog:warn

Active database connection methods:
  tcp:IP:PORT              PORT at remote IP
  ssl:IP:PORT              SSL PORT at remote IP
  unix:FILE                Unix domain socket named FILE
Passive database connection methods:
  ptcp:PORT[:IP]           listen to TCP PORT on IP
  pssl:PORT[:IP]           listen for SSL on PORT on IP
  punix:FILE               listen on Unix domain socket FILE
PKI configuration (required to use SSL):
  -p, --private-key=FILE   file with private key
  -c, --certificate=FILE   file with certificate for private key
  -C, --ca-cert=FILE       file with peer CA certificate

Other options:
  -h, --help                 display this help message
  -V, --version              display version information
```

```
admin@PICOS-OVS:~$
```

See ovs-vsctl main page for detailed syntax and additional information.

```
admin@Switch$man ovs-vsctl
ovs-vsctl(8)                                Open vSwitch Manual                                ovs-vs
NAME
       ovs-vsctl - utility for querying and configuring ovs-vswitchd
SYNOPSIS
       ovs-vsctl [options] -- [options] command [args] [-- [options] command [args]]...
DESCRIPTION
       The  ovs-vsctl  program  configures ovs-vswitchd(8) by providing a high-level interface to its configuration
       base.  See ovs-vswitchd.conf.db(5) for comprehensive documentation of the database schema.
       ovs-vsctl connects to an ovsdb-server process that maintains an Open vSwitch configuration database.   Using
       connection, it queries and possibly applies changes to the database, depending on the supplied commands.  Th
       it applied any changes, by default it waits until ovs-vswitchd has finished reconfiguring itself before it
       (If you use ovs-vsctl when ovs-vswitchd is not running, use --no-wait.)
       ovs-vsctl  can  perform any number of commands in a single run, implemented as a single atomic transaction a
       the database.
       The ovs-vsctl command line begins with global options (see OPTIONS below for details).   The  global  option
       followed by one or more commands.  Each command should begin with -- by itself as a command-line argument, t
       arate it from the following commands.  (The -- before the first command is optional.)  The command  itself
       with  command-specific  options,  if  any, followed by the command name and any arguments.  See EXAMPLES bel
       syntax examples.
   Linux VLAN Bridging Compatibility
       The ovs-vsctl program supports the model of a bridge implemented by Open vSwitch, in which a  single  bridge
       ports  ports  on  multiple  VLANs.   In  this model, each port on a bridge is either a trunk port that poten
       passes packets tagged with 802.1Q headers that designate VLANs or it is assigned a single implicit  VLAN  th
       never tagged with an 802.1Q header.
       For  compatibility  with  software designed for the Linux bridge, ovs-vsctl also supports a model in which t
       associated with a given 802.1Q VLAN is segregated into a separate bridge.  A special form of  the  add-br  c
       (see below) creates a ``fake bridge'' within an Open vSwitch bridge to simulate this behavior.  When such a
       bridge'' is active, ovs-vsctl will treat it much like a bridge separate from its ``parent bridge,'' but the
       implementation in Open vSwitch uses only a single bridge, with ports on the fake bridge assigned the implici
       of the fake bridge of which they are members.  (A fake bridge for VLAN 0 receives packets that have no 802.1
       or a tag with VLAN 0.)
<Some output omitted>
```


- Bridge Commands
  - ovs-vsctl add-br
  - ovs-vsctl del-br
  - ovs-vsctl list-br
  - ovs-vsctl set bridge
- Port Commands
  - ovs-vsctl add-port
  - ovs-vsctl list-ports
  - ovs-vsctl del-port
- Controller commands
- Database commands
- Interface commands
- Mirror Commands
- NetFlow Commands
- Open vSwitch commands
- Match-mode Command
- QoS_queue Commands
- sFlow commands
- Cos-map Command
- Egress-mode Command
- Set-flow-counter-mode Command
- Combinated-mode Command
- DSCP Commands

Bridge Commands

These commands are used to create and configure Open vSwitch bridges. Commands for displaying the status of OpenvSwitch bridges are also provided.

- ovs-vsctl add-br
- ovs-vsctl del-br
- ovs-vsctl list-br
- ovs-vsctl set bridge

ovs-vsctl add-br

To create a new bridge, use the **ovs-vsctl add-br** command. The new bridge initially has no ports, other than the bridge itself.

Syntax

ovs-vsctl [*options*] [**--may-exist**] **add-br** *bridge*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--may-exist	Without the **--may-exist** option, attempting to create bridge that already exists creates an error. With the **--may-exist** option, the command does nothing if the bridge already exists as a real bridge.
bridge	Arbitrary bridge name.

Examples

The following example creates a new bridge named **br0**:

```
admin@Switch$ovs-vsctl --may-exist add-br br0
```

ovs-vsctl del-br

To delete a bridge and all of its ports, use the **ovs-vsctl del-br** command. If the bridge is real, this command also deletes any fake bridges that were created with the bridge as parent, and all of their ports.

Syntax

ovs-vsctl [*options*] [**--if-exists**] **del-br** *bridge*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--if-exist	Without the **--if-exists** option, attempting to delete a bridge that does not exist creates an error. With the **--if-exists** option, attempting to delete a bridge that does not exist has no effect.
bridge	Name of the bridge to be deleted.

Examples

The following example deletes the bridge named **br0**:

```
admin@Switch$ovs-vsctl --if-exists del-br br0
```

ovs-vsctl list-br

To list all existing real and fake bridges, use the **ovs-vsctl list-br** command.

Syntax

ovs-vsctl [*options*] [**--real** | **--fake**] **list-br**

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--real	List only real bridges.
--fake	List only fake bridges.

Examples

The following example lists bridges, where only a single real bridge **br0** exists:

```
admin@Switch$ovs-vsctl list-br
br0
admin@Switch$ovs-vsctl --fake list-br
admin@Switch$ovs-vsctl --real list-br
br0
```

ovs-vsctl set bridge

Examples

The following examples provide typical usage of the **ovs-vsctl set bridge** command.

Disabling In-Band Management

By default, remote in-band management is enabled on Open vSwitch. You can disable in-band management by setting the **other-config** parameter **disable-in-band** to **true**. And the configurations will apply in all the controllers in the bridge.

The following example disables in-band management of bridge *br0*:

```
admin@Switch$ovs-vsctl set bridge br0 other-config:disable-in-band=true
```

The following example enables in-band management of bridge *br0*:

```
admin@Switch$ovs-vsctl set bridge br0 other-config:disable-in-band=false
```

Port Commands

ovs-vsctl *[--OPTION]* add-port *<bridge> <port> [ARG...] [--[OPTION] <COMMAND> [ARGs]]*

Add a new port named <*port*> to <*bridge*>. Including physic port, LAG port and GRE tunnel.

Physical Port

Example:

Add a physical port.

```
ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 trunks=2000,4094 -- set interface ge-1/1/1 type=pica8
```

Add a physical port and configure special link_speed.

```
ovs-vsctl add-port br0 te-1/1/49 vlan_mode=trunk tag=1 trunks=2000,4094 -- set interface te-1/1/49  type=pica8 opti
```

Crossflow Port

Example:

When adding a crossflow port the vlan_mode and the trunks should be set via CLI.

```
ovs-vsctl add-port br0 te-1/1/1 -- set interface te-1/1/1 type=crossflow
```

LAG Port

Example:

Add a lag interface:

```
root@PicOS-OVS#ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 trunks=2000,4094 -- set Interface ae1 type=pica8_la
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lag_type=static
```

Modify the numbers of the lag

```
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:members=ge-1/1/2,ge-1/1/3
```

LACP Port

Example:

Add a lacp port and configure the parameter.

```
root@PicOS-OVS#ovs-vsctl add-port br0 ae1 vlan_mode=trunk tag=1 trunks=2000,4094 -- set Interface ae1 type=pica8_la
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lag_type=lacp
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:members=ge-1/1/2,ge-1/1/3
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-system-id=00:11:11:11:11:11
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-system-priority=32768
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-time=fast
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-time=slow
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-mode=active
root@PicOS-OVS#ovs-vsctl set Interface ae1 options:lacp-mode=passive
root@PicOS-OVS#ovs-vsctl set Interface ge-1/1/2 options:lacp-port-id=2
root@PicOS-OVS#ovs-vsctl set Interface ge-1/1/2 options:lacp-port-priority=32768
```

```
root@PicOS-OVS#ovs-vsctl set Interface ge-1/1/2 options:lacp-aggregation-key=0
```

GRE Port

Example:

Add a GRE port.

```
ovs-vsctl add-port br0 gre1 -- set Interface gre1 type=pica8_gre options:remote_ip=10.10.61.10 options:local_ip=10.
```

ovs-vsctl *[--OPTION]* list-ports *<bridge>*

Print the names of all the ports on *<bridge>*.

Example:

```
ovs-vsctl list-ports br0
```

ovs-vsctl *[--OPTION]* del-port *<bridge>* *<port>*

Delete the port named *<port>* from *<bridge>*.

Example:

```
ovs-vsctl del-port br1 ge-1/1/1
```

ovs-vsctl *[--OPTION]* port-to-br *<port>*

Print name of the bridge which contrains the special *<port>*.

Example:

```
ovs-vsctl port-to-br ge-1/1/1
```

VXLAN Port

Example:

Add a VXLAN port.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 vxlan1 -- set interface vxlan1 type=pica8_vxlan options:remote_ip=10.10.10.2
```

L2GRE Port

Example:

Add a L2GRE port.

```
admin@PicOS-OVS$ovs-vsctl add-port br0 l2gre1 -- set interface l2gre1 type=pica8_l2gre options:remote_ip=10.10.61.1
```

- ovs-vsctl add-port
- ovs-vsctl list-ports
- ovs-vsctl del-port

ovs-vsctl add-port

To create a new port on the bridge from the network device of the same name, use the **ovs-vsctl add-port** command.

Syntax

ovs-vsctl [*options*] [**--may-exist**] **add-port** *bridge port* [*args*]

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced here.
--may-exist	Without the **--may-exist** option, attempting to create a port that exists is an error. With the **--may-exist** option, this command does nothing if the port already exists in the bridge and is not a bonded port.
bridge	Bridge name.
port	Port name.
args	Optional arguments configure additional parameters for the port. For example, tag=9 would make the port an access port for VLAN 9. The syntax is the same as that for the **ovs-vsctl set port** command.

Examples

The following example adds the ge-1/1/1 port to bridge br0:

```
admin@Switch$ovs-vsctl add-port br0 ge-1/1/1
```

Add Bond Ports

PicOS support bond multiple ports as in_port or output, and this virtual port will not influnce each physical port forwarding packets.

Examples

Bonding port ge-1/1/1 ~ ge-1/1/4 as one port.

```
// add ports
ovs-vsctl add-br br0 -- set bridge br0 datapath_type=pica8
ovs-vsctl add-port br0 ge-1/1/1 vlan_mode=trunk tag=1 -- set Interface ge-1/1/1 type=pica8
ovs-vsctl add-port br0 ge-1/1/2 vlan_mode=trunk tag=1 -- set Interface ge-1/1/2 type=pica8
ovs-vsctl add-port br0 ge-1/1/3 vlan_mode=trunk tag=1 -- set Interface ge-1/1/3 type=pica8
ovs-vsctl add-port br0 ge-1/1/4 vlan_mode=trunk tag=1 -- set Interface ge-1/1/4 type=pica8

// add bond ports
ovs-vsctl add-port br0 bond1 -- set Interface bond1 type=pica8_bond
ovs-vsctl set Interface bond1 options:members=ge-1/1/2,ge-1/1/3,ge-1/1/4

// add flows
ovs-ofctl add-flow br0 in_port=2049,actions=1
ovs-ofctl add-flow br0 in_port=1,actions=2049
```

ovs-vsctl list-ports

To list all of the ports within a bridge, use the **ovs-vsctl list-ports** command. The local bridge port is not included in the list.

Syntax

ovs-vsctl [*options*] **list-ports** *bridge*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced here.
bridge	Bridge name.

Examples

The following example lists ports within the bridge **br0**:

```
admin@Switch$ovs-vsctl list-ports br0
```

ovs-vsctl del-port

To create a new port on the bridge from the network device of the same name, use the **ovs-vsctl add-port** command.

Syntax

ovs-vsctl [*options*] [**--may-exist**] **del-port** *bridge port*

Parameters

options	See the output of **ovs-vsctl --help** command, also reproduced ovs−vsctl Commands.
--may-exist	Without the **--may-exist** option, attempting to create a port that exists is an error. With the **--may-exist** option, this command does nothing if the port already exists in the bridge and is not a bonded port.
bridge	Bridge name.
port	Port name.

Examples

The following example deletes the ge-1/1/1 port to bridge br0:

```
admin@Switch$ovs-vsctl del-port br0 ge-1/1/1
```

Controller commands

ovs-vsctl *[--OPTION]* set-controller *<bridge> <target> [target]*

Set the controllers for *<bridge>*. Support set multiple controllers at same time.
The bridge is typically configured to connect to multiple controllers. The controllers may select a primary controller that takes change of the flow tables of the bridge to inplement a network policy.
The <target> can use any of the following forms:

ovs-vsctl *[--OPTION]* set-controller *<bridge>* tcp:*<ip>*:*<port>*

Connect to controller with tcp port, the default value is 6633.
Example:

```
root@PicOS-OVS$ovs-vsctl set-controller br0 tcp:10.10.50.47:6633
```

ovs-vsctl *[--OPTION]* set-controller *<bridge>* ssl:*<ip>*:*<port>*

Connect to controller with specified SSL port, the default value is 6633.
Example:

```
root@PicOS-OVS$ovs-vsctl set-controller br0 ssl:10.10.50.100:6633
```

ovs-vsctl *[--OPTION]* get-controller *<bridge>*

Print the controllers for *<bridge>*.
Example:

```
ovs-vsctl get-controller br0
```

ovs-vsctl *[--OPTION]* del-controller *<bridge>*

Delete the controllers for *<bridge>*.
Example:

```
ovs-vsctl del-controller br0
```

ovs-vsctl *[--OPTION]* set-fail-mode *<bridge> <mode>*

Set the fail-mode for *<bridge>* to *<mode>*.
The *<mode>* used in control flow table when controller failure setting. Support **standalone** and **secure** modes, the default mode is **secure** mode.
If set the mode is standalone, ovs-vswitchd will take over responsibility for setting up flows when connect to controller fail, and all flows in bridge will clear and there is a flow named "normal" to let the switch work as a L2 switch ; If fail-mode set to secure, ovs-vswitchd will not set up flows nor clear all flows. In secure mode, the packet is dropped default, in other word, there is no flow named "normal" to let switch work as a L2 switch
Example:

```
ovs-vsctl set-fail-mode br0 standalone
```

ovs-vsctl *[--OPTION]* get-fail-mode *<bridge>*

Print the fail-mode for *<bridge>*. If not set the fail-mode, will print nothing.
Example:

```
ovs-vsctl get-fail-mode br0
```

ovs-vsctl *[--OPTION]* del-fail-mode *<bridge>*

Delete the fail-mode for *<bridge>*. After delete current mode will return the default mode standalone.
Example:

```
ovs-vsctl del-fail-mode br0
```

Database commands

Database commands create, list and modify the contents of ovsdb tables.PicOS OVS support the following tables, as:

Bridge table

Configure a bridge within an Open vSwitch. Record bridge configurations by _uuid in bridge tables.

Controller table

Configure an OpenFlow controller, record controller infos by _uuid in controller table.

Interface table

Configure a network device attached to a port, record interface configurations by _uuid in interface table.

Mirror table

Configure a mirror port to a bridge, record mirror configurations by _uuid in mirror table.

Open_vSwitch table

The global configurations for ovs-vswitchd, record configurations by _uuid.

Pica8 table

Pica_match_mode table

Port table

Configure bridge ports, record port configurations by _uuid in port table.

QoS table

Configure quality-of-service for a port, record QoS configurations by _uuid in QoS table.

Queue table

Configure one queue within a QoS, record by _uuid in queue table.

SSL table

sFlow table

Configure an sFlow exporter attached to a bridge, record by _uuid in sFlow table.

NetFlow table

Configure a NetFlow attached to a bridge, records by _uuid in NetFlow table.

ovs-vsctl *[--OPTION]* list *<table> [record]*

List the *[record]* record if special *[record]*, otherwise, list all records in *<table>.*
The *[record]* mean _uuid or special name
Examples:

```
admin@XorPlus$ovs-vsctl list port te-1/1/1
_uuid               : e16c6743-999e-49af-8c0a-bc27eb897924
bond_downdelay      : 0
bond_fake_iface     : false
bond_mode           : []
bond_updelay        : 0
external_ids        : {}
fake_bridge         : false
interfaces          : [d8674864-22f1-41eb-8ece-ce35d90c5a64]
lacp                : []
mac                 : []
name                : "te-1/1/1"
other_config        : {}
qos                 : []
statistics          : {}
status              : {}
tag                 : []
trunks              : []
vlan_mode           : []
```

```
admin@XorPlus$ovs-vsctl list bridge
_uuid               : 2fa9c8d9-055e-4c2a-b5e4-2f22505cbda6
controller          : [07e2aaf5-fca3-4f77-93fe-e726d58637b9]
datapath_id         : "5e3e00e09500169a"
datapath_type       : "pica8"
external_ids        : {}
fail_mode           : []
flood_vlans         : []
flow_tables         : {}
ipfix               : []
lldp_enable         : false
mirrors             : []
name                : "br0"
netflow             : []
other_config        : {}
ports               : [3b4d71fc-eaad-4b01-9b95-be56239f3253, 630fb94c-4a7c-42f7-a195-49fd9f525177, e16c6743-999e-49
protocols           : ["OpenFlow13"]
sflow               : []
status              : {}
stp_enable          : false
```

```
admin@XorPlus$ovs-vsctl list Pica8
_uuid               : 8570c5d9-b22d-40ed-9e84-1c7e3b0e1dfd
combinate_actions_enable: false
cos_map_enable      : true
egress_mode_enable  : false
egress_mode_table   : 0
flow_counter_mode   : []
hardware_type       : "P5401"
l2_l3_buffer_mode   : []
l2_l3_preference    : false
l2_mode_enable      : false
l2_mode_table       : 0
l2gre_key_length    : []
l3_ecmp_max_ports   : 0
l3_mode_enable      : false
l3_mode_table       : 0
lag_advance_hash_mapping_fields: []
loopback_enable     : false
match_mode          : []
port_mode           : max
proxy_arp_subnet    : []
proxy_icmpv6_subnet : []
udf_mode            : []
xovs_crossflow_ports: ["te-1/1/1", "te-1/1/2", "te-1/1/3", "te-1/1/4"]
xovs_openflow_ports : []
xovs_vlans          : ["1", "100-110"]
```

ovs-vsctl *[--OPTION]* find *<table> <condition> [condition…]*

List records satisfying *<condition>* in *<table>*.
The *<condition>* represent a column equels value or not. If the value is specified, the operations can be support: "=", "!=", "<", ">", "<=", ">=", "\{=\}", "\{!=}", "{<}", "{>}", "{<=}" and "{>=}".
Example:

```
ovs-vsctl find bridge datapath_id=5e3e089e01616580 name=br0
```

ovs-vsctl *[--OPTION]* get *<table> <record > <column> [:key]*

Print values of column in *<record>* in *<table>*. *<table>* mean table name, and *<record>* mean _uuid.
Example:(print the value of datapath_id in the _uuid=80984dfb-5f63-45c8-bd3f-6bda918ffc75 in bridge table.)

```
ovs-vsctl get bridge 80984dfb-5f63-45c8-bd3f-6bda918ffc75 datapath_id
```

ovs-vsctl *[--OPTION]* set *<table> <record > <column> [:key] <=value>*

Set or change the column values in <*record*> in <*table*>.
Example: (change the value of trunks in ge-1/1/2 in port table.)

```
root@PicOS-OVS$ovs-vsctl list port ge-1/1/2
_uuid : 6e7b862a-6503-4f1b-982d-b33b65e3dc01
bond_downdelay : 0
bond_fake_iface : false
bond_mode : []
bond_updelay : 0
external_ids : {}
fake_bridge : false
interfaces : [f1b5568f-bd6f-480d-a9ca-636486f387c2]
lacp : []
mac : []
name : "ge-1/1/2"
other_config : {}
qos : []
statistics : {}
status : {}
tag : 1
trunks : [2000, 4094]
root@PicOS-OVS$ovs-vsctl set port 6e7b862a-6503-4f1b-982d-b33b65e3dc01 trunks=100,200
root@PicOS-OVS$ovs-vsctl list port ge-1/1/2
_uuid : 6e7b862a-6503-4f1b-982d-b33b65e3dc01
bond_downdelay : 0
bond_fake_iface : false
bond_mode : []
bond_updelay : 0
external_ids : {}
fake_bridge : false
interfaces : [f1b5568f-bd6f-480d-a9ca-636486f387c2]
lacp : []
mac : []
name : "ge-1/1/2"
other_config : {}
qos : []
statistics : {}
status : {}
tag : 1
trunks : [100, 200]
vlan_mode : trunk
```

ovs-vsctl *[--OPTION]* destroy *<table> <record>*

Deletes<record> from <table>.

ovs-vsctl *[--OPTION]* add *<table> <record > <column> [key=] <value>*

Add the column values in <*record*> in <*table*>.
Example: (add the value of trunks in ge-1/1/2 in port table.)

```
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[100, 200]
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl add port ge-1/1/2 trunks 100,300
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[100, 200, 300]
```

ovs-vsctl *[--OPTION]* remove *<table> <record > <column> [key=] <value>*

Remove the column value in <*record*> in <*table*>.
Example: (remove the value of trunks in ge-1/1/2 in port table.)

```
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[100, 200, 300]
root@PicOS-OVS$ovs-vsctl remove port ge-1/1/2 trunks trunks 100
root@PicOS-OVS$
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[200, 300]
```

ovs-vsctl *[--OPTION]* clear *<table> <record > <column>*

Clear all values from column in <record> in <table>.
Example:
Clear all values of trunks in ge-1/1/2 in port table.

```
root@PicOS-OVS$ovs-vsctl get port ge-1/1/2 trunks
[200, 300]
root@PicOS-OVS$ovs-vsctl clear port ge-1/1/2 trunks
[]
root@PicOS-OVS$
```

Interface commands

ovs-vsctl *[--OPTION]* list-ifaces *<bridge>*

Print the names of all interfaces on <*bridge*>.
Example:

```
ovs-vsctl list-ifaces br0
```

ovs-vsctl *[--OPTION]* iface-to-br *<interface>*

Print the name of bridge that contains <*port*>.
Example:

```
ovs-vsctl iface-to-br ge-1/1/1
```

Mirror Commands

Chips mirror actions:

PRONTO3290 PRONTO3296 PRONTO3295(TR2)(egress mirror=true)
PRONTO3780 PRONTO3920 PRONTO3922 PRONTO3930 PRONTO3960 PRONTO3965 PRONTO3980 PRONTO3920 PRONTO3924(TD)

ES4654 AS4610_54P AS4610_54T AS4610_30P AS4610_30T(Helix4)(egress mirror=true)
PRONTO5101 PRONTO5401 AS6701_32X N2632XL N2948_6XL AS6712_32X AS5712_54X S4048 ARCTICA4806XP(TD2)

AS5812_54T AS5812_54X(TD2P)
DCS7032Q28 AS7712_32X Z9100 (TH)

Note：Egress mirror works correctly only on those switches that the parameter 'egress mirror' is true.According to above chips,3290 (Firebolt3),3296(Triumph2),helix4 support egress mirror.On other switches,the mirror port' traffics' action are not certain.

Below is the test result on some kinds of chips:

p3290(Firebolt3):

module name	mirror dst traffic test result
multitable	pass
udf/ttp multicast	pass
push mpls/pop mpls	failed(3290 do not support mpls)
egress mode	pass
flow control	pass

l2mpls	failed(3290 do not support mpls)

p3297(trumph2):

module name	mirror dst traffic test result
multitable	pass
ttp multicast	pass
udf/push mpls/pop mpls	pass
egress mode	pass
flow control	mirror test pass
l2mpls	pass

as5812_54t(trident2plus):

module name	mirror dst traffic test result
multitable	pass
ttp multicast	failed
udf/push mpls/pop mpls	pass
egress mode	pass
flow control	mirror test pass
l2mpls	failed(mirror port packets has one more vlan 4095)

vxlan/l2gre/NAT	pass

p6701(trident2):

module name	mirror dst traffic test result
multitable	pass

ttp multicast	failed
udf/push mpls/pop mpls	pass
egress mode	pass
flow control	pass
l2mpls/nat	pass

vxlan/l2gre	failed

p3920(trident+):

module name	mirror dst traffic test result
multitable	pass
ttp multicast	failed
udf/push mpls/pop mpls	pass
egress mode	pass
flow control	pass
l2mpls	pass

4610_54t_b(helix4):

module name	mirror dst traffic test result
multitable	pass
ttp multicast /udf	pass
push mpls/pop mpls	failed(4610 do not support mpls)
egress mode	pass
flow control	pass
l2mpls	failed(4610 do not support l2mpls)

as7712_32x(tomhark):

module name	mirror dst traffic test result
multitable	pass
ttp multicast	failed
pop mpls/udf	failed(do not support mpls)
egress mode	pass
flow control /l2mpls/nat/push mpls(ip packets)	pass
vxlan/l2gre	failed

Create One Mirror

ovs-vsctl [--OPTION] -- set bridge <bridge> mirrors=@m -- --id=@<port1> get Port <port1> -- --id=@<port2> get Port <port2> [-- --id=@<port3> get Port <port3>]-- --id=@m create Mirror name=<mirror-name> select-src-port=@<port1>[,@<port3>] select-dst-port=@<port1> [,@<port3>] output-port=@<port2>

PicOS OVS supports mirroring, **select-src-port** and **select-dst-port** represent the source ports of mirroring, **select-dst-port** means some packets (in switch chip) will go-out from the specified port (egress); **select-src-port** means some packets will enter the specified port (ingress); **output_port** means the monitor port. PicOS OVS supports up to 4 mirrors.

Before PicOS2.10 ovs only support configure physical port as output_port, from PicOS2.10 ovs also support lag interface as output_port.

Example1:
Add port ge-1/1/1, ge-1/1/2 and ge-1/1/3 to mirror, ge-1/1/1 and ge-1/1/2 as ingress and egress, the output port is ge-1/1/3.

```
root@PicOS-OVS$ovs-vsctl set bridge br0 mirrors=@m -- --id=@ge-1/1/1 get Port ge-1/1/1 -- --id=@ge-1/1/2 get Port g
```

Example2:
Add port ge-1/1/1, ge-1/1/2 and ae1 to mirror, ge-1/1/1 and ge-1/1/2 as ingress and egress, the output port is ae1.

```
root@PicOS-OVS$ovs-vsctl set bridge br0 mirrors=@m -- --id=@ge-1/1/1 get Port ge-1/1/1 -- --id=@ge-1/1/2 get Port g
```

ovs-vsctl *[--OPTION]* destroy *<table> <record>* – clear Bridge *<bridge>* mirrors

Example:

Delete a mirror named mymirror from mirror table in bridge br0.

```
admin@PicOS-OVS$ ovs-vsctl destroy Mirror mymirror -- clear Bridge br0 mirrors
or
admin@PicOS-OVS$ ovs-vsctl clear Bridge br0 mirrors
```

Create Two Mirrors

```
admin@PicOS-OVS$ovs-vsctl  -- set bridge br-s mirrors=@m,@m1 -- --id=@ge-1/1/1 get Port ge-1/1/1 -- --id=@ge-1/1/3
```

Add one mirror and monitor port is lag

```
admin@PicOS-OVS$ovs-vsctl -- add bridge br-s mirrors @m -- --id=@te-1/1/1 get Port te-1/1/1 -- --id=@te-1/1/2 get P
```

Delete one mirror

```
admin@PicOS-OVS$ovs-vsctl remove bridge br0 mirrors 76fd4479-67e9-4c65-8edb-b99d8706d8f9
```

NetFlow Commands

ovs-vsctl set Bridge <*bridge*> netflow=@nf -- --id=@nf create NetFlow targets=<*target*> active-timeout=<*timeout*>

Example:

```
admin@PicOS-OVS$ovs-vsctl set Bridge br0 netflow=@nf -- --id=@nf create NetFlow targets=\"10.10.50.207:5566\" activ
In the above CLI, the parametersare shown as following:
COLLECTOR_IP=10.10.50.207
COLLECTOR_PORT=5566
ACTIVE_TIMEOUT=30
```

ovs-vsctl – clear Bridge <*bridge*> netflow

Delete NetFlow from NetFlow table.

Example:
Clear NetFlow from NetFlow table in bridge br0.

```
admin@PicOS-OVS$ovs-vsctl -- clear Bridge br0 netflow
```

Open vSwitch commands

ovs-vsctl init (the command is not effect)

To initialize the Open vSwitch database if not yet initialized. If the database has already been initialized, the init command will have no effect.

ovs-vsctl show

Print a brief overview of database contents.

ovs-vsctl emer-reset

Reset the configurarion to clean state. Using this command can delete fail mode, OpenFLow controllers, port mirrors, NetFlow, sFlow, and IPFIX configuration.

Match-mode Command

ovs-vsctl *[--OPTION]* set-match-mode *<mode:options=priority> [mode:options=priority]*

By default, 2 TCAM entries are used to support all matching tuples for all flows, even if the flow does not use all matching tuples. To optimize the TCAM usage, PicOS-2.1 allows user to configure the switch in short flow TCAM match mode, in which, each flow will only consume 1 TCAM entry. To use this feature, the flow must use the exact fields described below and cannot mix fields from various modes:

When this mode is enabled (with the set-match-mode command), only specific fields can be used in the priority range defined by the command.

From PicOS2.9.0,add a new group(ipv4_quintuple group) for tomahawk platform besides the normal match mode groups supported by other platforms.

The flows must use the exact fields described below:

mac mode: "in_port,dl_src,dl_dst,dl_vlan,dl_type"

ip mode: "in_port,nw_proto,nw_src,nw_dst,tp_src,tp_dst,dl_type=0x0800"

arp_tpa mode: "in_port, arp_tpa, dl_type=0x0806"

ipv6_full mode: "in_port,dl_vlan,ipv6_src,ipv6_dst,tp_src,tp_dst,nw_proto,dl_type=0x86dd"

ipv6_src mode: "in_port,dl_src,dl_dst,dl_vlan,ipv6_src,nw_proto,dl_type=0x86dd"

ipv6_dst mode: "in_port,dl_src,dl_dst,dl_vlan,ipv6_dst,nw_proto,dl_type=0x86dd"

ipv4_quintuple: "in_port,dl_vlan,nw_src,nw_dst,tp_src,tp_dst,nw_proto,dl_type=0x0800"

For example, if mac mode is enabled, all the flows must only use one or more fields defined in the mac mode. If mac and ip modes are enabled, then you can configure either mac flows or ip flows based on the fields described above. However, you cannot mix the fields from mac and ip (that is, dl_src and nw_src)

Each mode is configured with a priority range that determines the flow priority. The flow priority must be specified when user configures the flow through ovs commands or controller.
If user does not want match-mode, configure match-mode as default. The default value is default.

Example:

Configure match-mode mac priority from 200 to 499; ip priority 500-999; arp_tpa priority 1000-2000.

```
root@PicOS-OVS$ovs-vsctl set-match-mode mac=10-1000,ip=2000-20000,arp_tpa=30000-40000,ipv6_full=50000-50001,ipv6_ds
```

Remove match-mode configuration.

```
root@PicOS-OVS$ ovs-vsctl set-match-mode [default]
```

ovs-vsctl show-match-mode

Print current match-mode.

Example:

```
admin@PicOS-OVS$ovs-vsctl show-match-modecurrent match modes:
 ipv4_quintuple:
   priorities={60001-65535}
   fields={in_port,dl_vlan,nw_src,nw_dst,tp_src,tp_dst,nw_proto,dl_type=0x0800}
 ipv6_src:
   priorities={50004-60000}
   fields={in_port,dl_src,dl_dst,dl_vlan,ipv6_src,nw_proto,dl_type=0x86dd}
 ipv6_dst:
   priorities={50002-50003}
   fields={in_port,dl_src,dl_dst,dl_vlan,ipv6_dst,nw_proto,dl_type=0x86dd}
 ipv6_full:
   priorities={50000-50001}
   fields={in_port,dl_vlan,ipv6_src,ipv6_dst,tp_src,tp_dst,nw_proto,dl_type=0x86dd}
 arp_tpa(both):
   priorities={30000-40000}
   fields={in_port,arp_tpa,dl_type=0x0806}
 mac:
   priorities={10-1000}
   fields={in_port,dl_src,dl_dst,dl_vlan,dl_type}
 ip:
   priorities={2000-20000}
   fields={in_port,nw_proto,nw_src,nw_dst,tp_src,tp_dst,dl_type=0x0800}
```

QoS_queue Commands

ovs-vsctl [--OPTION] -- set port <port> qos=@newqos -- --id=@newqos create qos type=PRONTO_STRICT queues:<queueid>=@newqueue [queues:<queueid>=@newqueue1] -- --id=@newqueue create queue other-config:min-rate=<minrate> other-config:max-rate=<maxrate> [-- --id=@newqueue1 create queue other-config:min-rate=<minrate> other-config:max-rate=<maxrate>]

Queue 0~7 represent priority 0~7, respectively.

Example:
Configure qos contain two queues: queue 0 and queue 7. And min and max rate of queue 0 and queue 7 is set as 10M.

```
admin@PicOS-OVS$ovs-vsctl set port ge-1/1/3 qos=@newqos -- --id=@newqos create qos type=PRONTO_STRICT queues:0=@new
```

ovs-vsctl *[--OPTION]* clear port *<port>* qos

Delete QoS applied *<port>*.

Example:
Clear QoS and queues applied port ge-1/1/3 from Qos table and queue table.

```
admin@PicOS-OVS$ovs-vsctl clear port ge-1/1/3 qos
admin@PicOS-OVS$ovs-vsctl --all destroy qos
admin@PicOS-OVS$ovs-vsctl --all destroy queue
```

sFlow commands

ovs-vsctl -- --id=@s create sFlow agent=<*agent*> target=<*target*>[,<*target*>,...] header=<*header*> samping=<*samping*> polling=<*polling*> -- set Bridge <*bridge*> sflow=@s

PicOS OVS supports sFlow v5.
Example:

```
admin@PicOS-OVS$ovs-vsctl -- --id=@s create sFlow agent=eth0 target=\"10.10.50.207:9901\" header=128 sampling=2000
In the above CLI, the parameters are shown as following:
COLLECTOR_IP=10.10.50.207
COLLECTOR_PORT=9901
AGENT_IP=eth0
HEADER_BYTES=128
SAMPLING_N=64
POLLING_SECS=10
```

ovs-vsctl – clear Bridge <*bridge*> sflow

Delete sFlow from sFlow table.
Example:
Clear sFlow from sFlow table in bridge br0.

```
admin@PicOS-OVS$ovs-vsctl -- clear Bridge br0 sflow
```

Troubleshoot the configuration

```
admin@5712$ovs-vsctl list sflow
_uuid               : 3362a543-4a1a-47db-898a-0ec0eddb7aa0
agent               : "eth0"
external_ids        : {}
header              : 128
polling             : 30
sampling            : 2000
targets             : ["172.16.0.173:8008"]
```

Cos-map Command

ovs-vsctl set-cos-map <*TRUE|FALSE*>

From Picos-2.6, user can enable/disable the cos-mapping, the default value is disabled. Once cos-mapping is enabled, the packet with the different cos value is mapped to queue0-7.
Usage:

```
Enable/Disable:
 ovs-vsctl set-cos-map true
 ovs-vsctl set-cos-map false

Set dscp map on port:
 ovs-vsctl set interface ge-1/1/1 dscp_map=0=q1,1=q1,2=q2
 equal to:
 ovs-vsctl set interface ge-1/1/1 dscp_map:0=q1 dscp_map:1=q1 dscp_map:2=q2

 Note:
  dscp range is [0, 63];
  queue range value is {q0, q1, q2, q3, q4, q5, q6, q7};
  if a dscp value is not configured, the default queue is q0.

Clear all dscp map on port:
 ovs-vsctl clear interface ge-1/1/1 dscp_map

 Note:
 if no dscp_map configuration, the default map is:

       dscp   queue
    --------  -----
     0 -  7:   q0
     8 - 15:   q1
    16 - 23:   q2
    24 - 31:   q3
    32 - 39:   q4
    40 - 47:   q5
    48 - 55:   q6
    56 - 63:   q7
```

ovs-vsctl show-cos-map

Display the configuration of cos-mapping.
Example:

```
admin@PicOS-OVS$ovs-vsctl show-cos-map
cos mapping: enabled

admin@PicOS-OVS$ovs-vsctl show-cos-map ge-1/1/1
cos mapping: enabled
{
       dscp   queue
    --------  -----
     0 -  7:   q0
     8 - 15:   q1
    16 - 23:   q2
    24 - 31:   q3
    32 - 39:   q4
    40 - 47:   q5
    48 - 55:   q6
    56 - 63:   q7
}
```

Egress-mode Command

ovs-vsctl enable-egress-mode <*TRUE|FALSE*> *[TABLE]*

Enable or disable egress-mode.

If not specified the [TABLE], use table 253 to support another 256 flow, the action of flow should be drop or mod_nw_tos.

eg. The valid table is from 1 to 253, except the table 250, it is used by udf-mode.

> ⚠ egress-mode cannot be configured on the table which has configured L2/L3 mode.

Enable egress-mode on default table or specify table:

```
ovs-vsctl set-egress-mode TRUE
ovs-vsctl set-egress-mode TRUE 251
```

Add flow in egress-mode table:

```
ovs-ofctl add-flow br0 table=253,in_port=1,actions=drop
ovs-ofctl add-flow br0 table=253,dl_type=0x0800,nw_dst=192.168.1.3,actions=mod_nw_tos:16
```

ovs-vsctl show-egress-mode

Show the current configuration of egress-mode.

Set-flow-counter-mode Command

ovs-vsctl set-flow-counter-mode <bytes|packets|both>

Set the flow counter type.
Example:

```
admin@PicOS-OVS$ovs-vsctl set-flow-counter-mode bytes

  Please reboot for the change to take effect!

admin@PicOS-OVS$sudo systemctl restart picos
..............
admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=50000
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=meter:1,output:14
admin@PicOS-OVS$ovs-vsctl show-flow-counter-mode
Flow Stats Counter Mode:
  Bytes mode is enabled
  Packets mode is disabled

admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=21.563s, table=0, n_packets=n/a, n_bytes=0, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:n/a byte_in_count:0 duration:27.266s bands:
0: packet_count:n/a byte_count:0
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:n/a byte_in_count:151400 duration:33.138s bands:
0: packet_count:n/a byte_count:151400
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=34.288s, table=0, n_packets=n/a, n_bytes=151400, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$

admin@PicOS-OVS$ovs-vsctl set-flow-counter-mode packets

  Please reboot for the change to take effect!

admin@PicOS-OVS$sudo systemctl restart picos
..............
admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=50000
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:0 byte_in_count:n/a duration:12.306s bands:
0: packet_count:0 byte_count:n/a
admin@PicOS-OVS$ovs-vsctl show-flow-counter-mode
Flow Stats Counter Mode:
  Bytes mode is disabled
  Packets mode is enabled

admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:0 byte_in_count:n/a duration:24.705s bands:
0: packet_count:0 byte_count:n/a
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:100 byte_in_count:n/a duration:29.904s bands:
0: packet_count:100 byte_count:n/a
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=38.496s, table=0, n_packets=100, n_bytes=n/a, in_port=1 actions=meter:1,output:14
```

```
admin@PicOS-OVS$

admin@PicOS-OVS$ovs-vsctl set-flow-counter-mode both

  Please reboot for the change to take effect!
admin@PicOS-OVS$sudo systemctl restart picos

..............
admin@PicOS-OVS$ovs-vsctl show-flow-counter-mode
Flow Stats Counter Mode:
  Bytes mode is enabled
  Packets mode is enabled

admin@PicOS-OVS$ovs-ofctl add-meter br0 meter=1,kbps,band=type=drop,rate=50000
admin@PicOS-OVS$ovs-ofctl add-flow br0 in_port=1,actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:0 byte_in_count:0 duration:11.138s bands:
0: packet_count:0 byte_count:0
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=12.808s, table=0, n_packets=0, n_bytes=0, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl dump-flows br0
OFPST_FLOW reply (OF1.4) (xid=0x2):
 cookie=0x0, duration=18.345s, table=0, n_packets=100, n_bytes=151400, in_port=1 actions=meter:1,output:14
admin@PicOS-OVS$ovs-ofctl meter-stats br0
OFPST_METER reply (OF1.4) (xid=0x2):
meter:1 flow_count:1 packet_in_count:100 byte_in_count:151400 duration:24.802s bands:
0: packet_count:100 byte_count:151400
admin@PicOS-OVS$
```

Combinated-mode Command

ovs-vsctl set-combinated-mode <*TRUE*|*FALSE*>

Enable combinated mode to deal with VCAP/ICAP flow conflict, only half of TCAM flow number can be used.

ovs-vsctl show-combinated-mode

Show whether combinated-mode is enabled or not.

DSCP Commands

DSCP (Differentiated Services Code Point) is a field in the header of an IP packet that is used to provide QoS (Quality of Service). You can mark each packet with a DSCP code and assign to it the corresponding level of service. PicOS 2.6 enables users to map a specific DSCP value to an interface queue. If you do not configure DSCP mappings, PicOS 2.6 uses the following defaults:

DSCP Values	Queue
0-7	q0
8-15	q1
16-23	q2
24-31	q3
32-39	q4
40-47	q5
48-55	q6

The following command is used to enable or disable DSCP mapping:

ovs-vsctl set-cos-map <**true** | **false**>

By default, DSCP mapping is disabled in PicOS 2.6. Once DSCP mapping is enabled, packets with different DSCP values are placed in different queues (q0-q7).

The following example enables DSCP mapping:

ovs-vsctl set-cos-map true

The following example disables DSCP mapping:

ovs-vsctl set-cos-map false

The default DSCP map for interface **ge-1/1/1** can be modified as shown below:

ovs-vsctl set interface ge-1/1/1 dscp_map=0=q1,1=q1,2=q2

An alternative method would be to use the following command:

ovs-vsctl set interface ge-1/1/1 dscp_map:0=q1, dscp_map:1=q1 dscp_map:2=q2

DSCP values range from 0 to 63. The available queues are q0, q1, q2, q3, q4, q5, q6, and q7. If a DSCP value is not configured, the default queue is q0. Incoming packets with any DSCP values will be treated the same.

Use the following command to clear the DSCP map of an interface:

ovs-vsctl clear interface ge-1/1/1 dscp_map

Use the following command to set the DSCP map of an interface:

ovs-vsctl set interface ge-1/1/1 dscp_map=0=q1,1=q1,2=q2

or

ovs-vsctl set interface ge-1/1/1 dscp_map:0=q1 dscp_map:1=q1 dscp_map:2=q2

You may use the following commands to show the DSCP map:

ovs-vsctl show-cos-map
ovs-vsctl show-cos-map ge-1/1/1