

IP Routing Commands

Оглавление

1. RIP COMMANDS	18
1.1. address-family	18
1.2. auto-summary	19
1.3. bdf all-interfaces	20
1.4. default-information originate	22
1.5. default-metric	23
1.6. distance	24
1.7. distribute-list in	26
1.8. distribute-list out	27
1.9. enable mib-binding	29
1.10. exit-address-family	30
1.11. fast-reroute	31
1.12. graceful-restart	32
1.13. ip rip authentication key-chain	34
1.14. ip rip authentication mode	36
1.15. ip rip authentication text-password	37
1.16. ip rip bfd	39
1.17. ip rip default-information	40
1.18. ip rip receive enable	41
1.19. ip rip receive version	42
1.20. ip rip send enable	44
1.21. ip rip send supernet-routes	45
1.22. ip rip send version	46
1.23. ip rip split-horizon	47
1.24. ip rip subvlan	49
1.25. ip rip summary-address	50
1.26. ip rip triggered	51
1.27. ip rip v2-broadcast	53
1.28. neighbor	54
1.29. network	55
1.30. offset-list	57
1.31. output-delay	58
1.32. passive-interface	59
1.33. redistribute	61
1.34. router rip	63

1.35. show ip rip	64
1.36. show ip rip database	66
1.37. show ip rip external	68
1.38. show ip rip interface	69
1.39. show ip rip peer	71
1.40. timers basic	72
1.41. validate-update-source	74
1.42. version	75
2. OSPFV2 COMMANDS	77
2.1. area	77
2.2. area authentication	78
2.3. area default-cost	79
2.4. area filter-list	80
2.5. area nssa	82
2.6. area range	84
2.7. area stub	86
2.8. area virtual-link	87
2.9. auto-cost	91
2.10. bdf all-interfaces	92
2.11. capability opaque	93
2.12. clear ip ospf process	94
2.13. compatible rfc1583	96
2.14. default-information originate	96
2.15. default-metric	99
2.16. discard-route	100
2.17. distance ospf	101
2.18. distribute-list in	102
2.19. distribute-list out	104
2.20. enable mib-binding	105
2.21. enable traps	107
2.22. fast-reroute	109
2.23. graceful-restart	111
2.24. graceful-restart helper	113
2.25. ip ospf authentication	114
2.26. ip ospf authentication-key	115
2.27. ip ospf bdf	117
2.28. ip ospf cost	118

2.29. ip ospf database-filter all out	119
2.30. ip ospf dead-interval	120
2.31. OSPF supports the Fast Hello function.	121
2.32. ip ospf disable all	122
2.33. ip ospf fast-reroute protection	123
2.34. ip ospf fast-reroute no-eligible-backup	125
2.35. ip ospf hello-interval	126
2.36. ip ospf message-digest-key	127
2.37. ip ospf mtu-ignore	129
2.38. ip ospf network	130
2.39. ip ospf priority	132
2.40. ip ospf retransmit-interval	133
2.41. ip ospf source-check-ignore	134
2.42. ip ospf subvlan	135
2.43. ip ospf transmit-delay	136
2.44. ispf enable	138
2.45. log-adj-changes	139
2.46. max-concurrent-dd	140
2.47. max-metric	141
2.48. neighbor	143
2.49. nsr	145
2.50. network area	146
2.51. overflow database	148
2.52. overflow database external	149
2.53. overflow memory-lack	151
2.54. passive-interface	152
2.55. redistribute	153
2.56. router ospf	156
2.57. router ospf max-concurrent-dd	157
2.58. router-id	158
2.59. show ip ospf	159
2.60. show ip ospf border-routers	165
2.61. show ip ospf database	166
2.62. show ip ospf interface	180
2.63. show ip ospf ispf	183
2.64. show ip ospf neighbor	185
2.65. show ip ospf route	188

2.66. show ip ospf spf	190
2.67. show ip ospf summary-address	191
2.68. show ip ospf topology	192
2.69. show ip ospf virtual-link	195
2.70. summary-address	197
2.71. timers lsa arrival	198
2.72. timers pacing lsa-group	199
2.73. timers pacing lsa-transmit	200
2.74. timers spf	202
2.75. timers throttle lsa all	203
2.76. timers throttle route	205
2.77. timers throttle spf	206
2.78. two-way-maintain	208
3. OSPFV3 COMMANDS	210
3.1. area authentication	210
3.2. area default-cost	211
3.3. area encryption	212
3.4. area nssa	214
3.5. area-range	216
3.6. area stub	217
3.7. area virtual-link	219
3.8. auto-cost	222
3.9. bdf all-interfaces	223
3.10. clear ipv6 ospf process	224
3.11. default-information originate	225
3.12. default-metric	227
3.13. distance	228
3.14. distribute-list in	229
3.15. distribute-list out	231
3.16. enable mib-binding	232
3.17. enable traps	233
3.18. graceful-restart	235
3.19. graceful-restart helper	237
3.20. ipv6 ospf area	238
3.21. ipv6 ospf authentication	240
3.22. ipv6 ospf bdf	241
3.23. ipv6 ospf cost	242

3.24. ipv6 ospf dead-interval	244
3.25. ipv6 ospf encryption	246
3.26. ipv6 ospf hello-interval	247
3.27. ipv6 ospf mtu-ignore	249
3.28. ipv6 ospf neighbor	250
3.29. ipv6 ospf network	251
3.30. ipv6 ospf priority	253
3.31. Command Mode	253
3.32. ipv6 ospf retransmit-interval	254
3.33. ipv6 ospf subvlan	255
3.34. ipv6 ospf transmit-delay	256
3.35. ipv6 router ospf	257
3.36. ipv6 router ospf max-concurrent-dd	258
3.37. log-adj-changes	259
3.38. max-concurrent-dd	260
3.39. passive-interface	261
3.40. redistribute	262
3.41. router-id	266
3.42. summary-prefix	268
3.43. show ipv6 ospf	269
3.44. show ipv6 ospf database	271
3.45. show ipv6 ospf interface	273
3.46. show ipv6 ospf neighbor	274
3.47. show ipv6 ospf restart	275
3.48. show ipv6 ospf route	276
3.49. show ipv6 ospf summary-prefix	277
3.50. show ipv6 ospf topology	278
3.51. show ipv6 ospf virtual-links	280
3.52. timers lsa arrival	281
3.53. timers pacing lsa-group	282
3.54. timers pacing lsa-transmit	283
3.55. timers spf	284
3.56. timers throttle lsa all	285
3.57. timers throttle route	287
3.58. timers throttle spf	288
3.59. two-way-maintain	290

4. IS-IS COMMANDS	292
4.1. address-family ipv6	292
4.2. adjacency-check	293
4.3. re-authentication	294
4.4. authentication key-chain	295
4.5. authentication mode	297
4.6. authentication send-only	298
4.7. bfd all-interfaces	300
4.8. clear clns neighbors	302
4.9. clear isis *	303
4.10. clear isis counter	304
4.11. default-information originate	304
4.12. distance	306
4.13. domain-password	306
4.14. enable mib-binding	308
4.15. enable traps	309
4.16. exit-address-family	310
4.17. graceful-restart	311
4.18. graceful-restart grace-period	312
4.19. graceful-restart helper disable	313
4.20. hello padding	314
4.21. hostname dynamic	315
4.22. ignore-lsp-errors	316
4.23. ip router isis	317
4.24. ipv6 router isis	318
4.25. isis authentication key-chain	319
4.26. isis authentication mode	321
4.27. isis authentication send-only	323
4.28. isis bfd	324
4.29. isis circuit-type	326
4.30. isis csnp-interval	327
4.31. isis hello-interval	329
4.32. isis hello-multiplier	330
4.33. isis hello padding	331
4.34. isis lsp-interval	332
4.35. isis mesh-group	333
4.36. isis metric	334

4.37. isis network point-to-point	336
4.38. isis password	337
4.39. isis priority	338
4.40. isis psnp-interval	339
4.41. isis retansmit-interval	340
4.42. isis subvlan	341
4.43. isis three-way-handshake disable	342
4.44. isis wide-metric	343
4.45. is-type	345
4.46. log-adjacency-changes	346
4.47. lsp-fragments-extend	346
4.48. lsp-gen-interval	348
4.49. lsp-length originate	350
4.50. lsp-length receive	351
4.51. lsp-refresh-interval	352
4.52. max-area-addresses	353
4.53. maximum-paths	354
4.54. max-lsp-lifetime	355
4.55. multi-topology	357
4.56. net	358
4.57. passive-interface	360
4.58. redistribute	361
4.59. redistribute isis level-1 into level-2	363
4.60. redistribute isis level-2 into level-1	365
4.61. router isis	367
4.62. set-overload-bit	368
4.63. spf-interval	371
4.64. summary-address	373
4.65. summary-prefix	374
4.66. two-way-maintain	375
4.67. virtual-system	376
4.68. show clns is-neighbors	378
4.69. show clns neighbors	380
4.70. show isis counter	381
4.71. show isis database	382
4.72. show isis graceful-restart	384
4.73. show isis hostname	386

4.74. show isis ipv6 topology	387
4.75. show isis interface	388
4.76. show isis mesh-groups	391
4.77. show isis neighbors	391
4.78. show isis virtual-neighbors	393
4.79. show isis protocol	394
4.80. show isis topology	396
5. BGP4 COMMANDS	398
5.1. address-family ipv4	398
5.2. address-family ipv4 vrf	399
5.3. address-family ipv6	400
5.4. address-family ipv6 vrf	401
5.5. address-family l2vpn	402
5.6. advertise ipv4 unicast	402
5.7. advertise ipv6 unicast	403
5.8. aggregate-address (IPv4)	404
5.9. bgp advertise non-transitive extcommunity	406
5.10. bgp always-compare-med	407
5.11. bgp asnotation dot	408
5.12. bgp bestpath as-path ignore	409
5.13. bgp bestpath as-path multipath-relax	410
5.14. bgp bestpath compare-confed-aspath	411
5.15. bgp bestpath compare-routerid	412
5.16. bgp bestpath med confed	413
5.17. bgp bestpath med missing-as-worst	414
5.18. bgp bestpath multipath-compare-routerid	415
5.19. bgp client-to-client reflection	416
5.20. bgp cluster-id	417
5.21. bgp confederation identifier	418
5.22. bgp confederation peers	420
5.23. bgp dampening	421
5.24. bgp default ipv4-unicast	423
5.25. bgp default local-preference	424
5.26. bgp default route-target filter	425
5.27. bgp enforce-first-as	427
5.28. bgp fast-external-fallover	428
5.29. bgp fast-reroute	429

5.30. bgp graceful-restart	430
5.31. bgp graceful-restart disable	431
5.32. bgp graceful-restart restart-time	432
5.33. bgp graceful-restart stalepath-time	433
5.34. bgp initial-advertise-delay	435
5.35. bgp log-neighbor-changes	436
5.36. bgp maxas-limit	437
5.37. bgp maximum-prefix	438
5.38. bgp mp-error-handle session-retain	439
5.39. bgp nexthop trigger delay	441
5.40. bgp nexthop trigger enable	442
5.41. bgp notify unsupport-capability	442
5.42. bgp redistribute-internal	443
5.43. bgp router-id	444
5.44. bgp scan-rib disable	445
5.45. bgp scan-time	446
5.46. bgp tcp-source-check disable	447
5.47. bgp timer accuracy-control	448
5.48. bgp update-delay	449
5.49. clear bgp all	450
5.50. clear bgp all peer-group	452
5.51. clear bgp all update-group	453
5.52. clear bgp ipv4 unicast	454
5.53. clear bgp ipv4 unicast dampening	455
5.54. clear bgp ipv4 unicast external	456
5.55. clear bgp ipv4 unicast flap-statistics	457
5.56. clear bgp ipv4 unicast peer-group	458
5.57. clear bgp ipv4 unicast table-map	459
5.58. clear bgp ipv4 unicast update-group	460
5.59. clear bgp ipv6 unicast	461
5.60. clear bgp ipv6 unicast dampening	463
5.61. clear bgp ipv6 unicast external	464
5.62. clear bgp ipv6 unicast flap-statistics	465
5.63. clear bgp ipv6 unicast peer-group	466
5.64. clear bgp ipv6 unicast table-map	467
5.65. clear bgp ipv6 unicast update-group	468
5.66. clear bgp l2vpn evpn	469

5.67. clear bgp l2vpn evpn dampening	470
5.68. clear bgp l2vpn evpn external	471
5.69. clear bgp l2vpn evpn flap-statistics	471
5.70. clear bgp l2vpn evpn peer-group	472
5.71. clear bgp l2vpn evpn update-group	473
5.72. clear evpn conflict mac	474
5.73. clear ip bgp	475
5.74. clear ip bgp dampening	477
5.75. clear ip bgp external	478
5.76. clear ip bgp flap-statistics	479
5.77. clear ip bgp peer-group	480
5.78. clear ip bgp table-map	481
5.79. clear ip bgp update-group	482
5.80. default-information originate	483
5.81. default-metric	484
5.82. distance bgp	485
5.83. evpn	486
5.84. export map(EVPN VNI)	488
5.85. import map(EVPN VNI)	489
5.86. maximum-paths	490
5.87. maximum-prefix	491
5.88. neighbor activate	493
5.89. neighbor advertisement-interval	494
5.90. neighbor allowas-in	495
5.91. neighbor as-originate-interval	496
5.92. neighbor default-originate	498
5.93. neighbor description	499
5.94. neighbor distribute-list	500
5.95. neighbor ebgp-multihop	501
5.96. neighbor fall-over bfd	502
5.97. neighbor filter-list	503
5.98. neighbor local-as	505
5.99. neighbor maximum-prefix	507
5.100. neighbor next-hop-self	508
5.101. neighbor next-hop-unchanged	509
5.102. neighbor password	510
5.103. neighbor peer-group (creating)	512

5.104. neighbor peer-group (assigning members)	513
5.105. neighbor prefix-list	515
5.106. neighbor remote-as	516
5.107. neighbor remove-private-as	517
5.108. neighbor route-map	518
5.109. neighbor route-reflector-client	520
5.110. neighbor send-community	521
5.111. neighbor shutdown	522
5.112. neighbor soft-reconfiguration inbound	523
5.113. neighbor timers	525
5.114. neighbor unsuppress-map	527
5.115. neighbor update-delay	528
5.116. neighbor version	530
5.117. neighbor weight	531
5.118. network	532
5.119. network synchronization	534
5.120. overflow memory-lack	535
5.121. rd	536
5.122. redistribute	538
5.123. redistribute ospf	539
5.124. redistribute isis	541
5.125. route-target	542
5.126. synchronization	545
5.127. table-map	546
5.128. timers bgp	547
5.129. how bgp all	548
5.130. show bgp all summary	549
5.131. show bgp ipv4 unicast	552
5.132. show bgp ipv4 unicast [vrf <i>vrf-name</i>] dampening dampened-paths	552
5.133. show bgp ipv4 unicast dampening parameters	557
5.134. show bgp ipv4 unicast neighbors	558
5.135. show bgp ipv4 unicast paths	559
5.136. show bgp ipv4 unicast summary	560
5.137. show bgp ipv4 unicast update-group	561
5.138. show bgp ipv6 unicast	563
5.139. show bgp ipv6 unicast dampening parameters	566
5.140. show bgp ipv6 unicast neighbors	567

5.141. show bgp ipv6 unicast paths	568
5.142. show bgp ipv6 unicast summary	569
5.143. show bgp ipv6 unicast update-group	569
5.144. show bgp l2vpn	571
5.145. show bgp l2vpn update-group	576
5.146. show bgp statistics	578
5.147. show evpn	580
5.148. show evpn mac	582
5.149. show ip bgp	584
5.150. vni	587
5.151. vni range	588
6. PBR COMMANDS	590
6.1. clear ip pbr statistics	590
6.2. clear ipv6 pbr statistics	591
6.3. ip local policy route-map	592
6.4. ip policy	594
6.5. ip policy route-map	595
6.6. ip policy-source in-interface	597
6.7. ipv6 local policy route-map	599
6.8. ipv6 policy	601
6.9. ipv6 policy route-map	603
6.10. ipv6 policy-source in-interface	605
6.11. show ip pbr bfd	607
6.12. show ip pbr route	608
6.13. show ip pbr route-map	611
6.14. show ip pbr source-route	612
6.15. show ip pbr statistics	615
6.16. show ip policy	616
6.17. show ipv6 pbr bfd	617
6.18. show ipv6 pbr route	618
6.19. show ipv6 pbr route-map	621
6.20. show ipv6 pbr source- route	622
6.21. show ipv6 pbr statistics	624
6.22. show ipv6 policy	625
7. VRF COMMANDS	627
7.1. address-family	627
7.2. description	628

7.3. exit-address-family	629
7.4. ip vrf	630
7.5. ip vrf forwarding	631
7.6. ip vrf receive	632
7.7. maximum routes	633
7.8. vrf definition	635
7.9. vrf forwarding	636
7.10. vrf receive	637
7.11. show ip vrf	639
7.12. show vrf	640
8. RIPNG COMMANDS	643
8.1. clear ipv6 rip	643
8.2. default-metric	644
8.3. distance	645
8.4. distribute-list	646
8.5. graceful-restart	647
8.6. ipv6 rip default-information	649
8.7. ipv6 rip enable	650
8.8. ipv6 rip metric-offset	651
8.9. ipv6 rip subvlan	652
8.10. ipv6 router rip	653
8.11. passive-interface	654
8.12. redistribute	655
8.13. show ipv6 rip	657
8.14. show ipv6 rip database	658
8.15. split-horizon	659
8.16. timers	661
9. NSM COMMANDS	663
9.1. clear ip route	663
9.2. ip default-network	664
9.3. ip fast-reroute route-map	665
9.4. ip route	666
9.5. ip route static bfd	669
9.6. ip route static inter-vrf	670
9.7. ip routing	671
9.8. ip static route-limit	672
9.9. ipv6 route	673

9.10. ipv6 route static bfd	675
9.11. ipv6 static route-limit	677
9.12. ipv6 unicast-routing	678
9.13. maximum-paths	679
9.14. show ip route	680
9.15. show ip route static bfd	684
9.16. show ip route summary	685
9.17. show ip route track-table	688
9.18. show ipv6 route	689
9.19. show ip route static bfd	691
9.20. show ipv6 route summary	692
10. PROTOCOL-INDEPENDENT COMMANDS	695
10.1. accept-lifetime	695
10.2. ip as-path access-list	696
10.3. ip community-list	697
10.4. ip extcommunity-list	698
10.5. ip prefix-list	700
10.6. ip prefix-list description	702
10.7. ip prefix-list sequence-number	703
10.8. ipv6 prefix-list	703
10.9. ipv6 prefix-list description	705
10.10. ipv6 prefix-list sequence-number	706
10.11. key	707
Use this command to define a key chain and enter the key chain configuration mode. Use	708
10.12. key-string	709
10.13. match as-path	710
10.14. match community	711
10.15. match extcommunity	712
10.16. match interface	714
10.17. match ip address	716
10.18. match ip next-hop	718
10.19. match ip route-source	720
10.20. match ipv6 address	722
10.21. match ipv6 next-hop	723
10.22. match ipv6 route-source	725
10.23. match metric	727

10.24. match origin	729
10.25. match route-type	730
10.26. match tag	732
10.27. memory-lack exit-policy	734
10.28. route-map	735
10.29. send-lifetime	738
10.30. set aggregator as	739
10.31. set as-path prepend	740
10.32. set atomic-aggregate	741
10.33. set comm-list delete	742
10.34. set community	743
10.35. set dampening	745
10.36. set extcomm-list delete	746
10.37. set extcommunity	748
10.38. set fast-reroute	749
10.39. set ip default next-hop	750
10.40. set ip dscp	752
10.41. set ip next-hop	753
10.42. set ip next-hop recursive	755
10.43. set ip next-hop verify-availability	757
10.44. set ip precedence	759
10.45. set ip tos	761
10.46. set ipv6 default next-hop	762
10.47. set ipv6 next-hop	764
10.48. set ipv6 next-hop verify-availability	766
10.49. set ipv6 precedence	768
10.50. set level	769
10.51. set local-preference	771
10.52. set metric	772
10.53. set metric-type	774
10.54. set next-hop	775
10.55. set origin	777
10.56. set originator-id	778
10.57. set tag	779
10.58. set weight	781
10.59. show ip as-path-access-list	782
10.60. show ip community-list	783

10.61. show ip extcommunity-list	784
10.62. show ip prefix-list	785
10.63. show ip protocols	786
10.64. show ipv6 prefix-list	788
10.65. show key chain	789
10.66. show route-map	790

1. RIP COMMANDS

1.1. address-family

Use this command to configure the RIP protocol in address family configuration sub-mode. Use the

no form of this command to restore the default setting.

`address-family ipv4 vrf vrf-name`

`no address-family ipv4 vrf vrf-name`

Parameter Description

Parameter	Description
vrf <i>vrf-name</i>	Specifies the VRF name associated with the sub-mode command.

Defaults

The address family of the RIP protocol is not configured by default.

Command Mode

Route configuration mode

Usage Guide

Use the address-family command to enter the address family configuration sub-mode. The prompt is (config-router-af) #. When you specify the VRF associated with the sub-mode for the first time, the RIP instance corresponding to the VRF will be created. In the sub-mode, you can configure the VRF RIP routing information.

To remove the address family sub-mode and return to the route configuration mode, use the

`exit-address-family` or `exit` command.

Configuration Examples

The following example creates a VRF with the name of vpn1 and creates its RIP instance.

```
QTECH(config)# ip vrf vpn1 QTECH(config-vrf)# exit
QTECH(config)# interface fastEthernet 1/0
QTECH(config-if-FastEthernet 0/1)# ip vrf forwarding vpn1
QTECH(config-if-FastEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 QTECH(config)#
router rip
QTECH(config-router)# address-family ipv4 vrf vpn1 QTECH(config-router)# network
```

192.168.1.0

QTECH(config-router)# exit-address-family

Related Commands

Command	Description
exit-address-family	Exits the address family configuration sub-mode.
ip vrf	Creates a VRF.

Platform Description

N/A

1.2. auto-summary

Use this command to enable automatic summary of RIP routes. Use the **no** form of this command to disable this function

auto-summary no auto-summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Automatic summary of RIP routes is enabled by default

Command Mode

Routing process configuration mode

Usage Guide

Automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classified network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.



Automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly.

Advertising the summarized route is more efficient than advertising individual routes in light of the following factors:

The summarized route is always processed preferentially when you query the RIP database.

Any sub-route is ignored when you query the RIP database, reducing the processing time.

If you want to learn the specific sub-routes instead of the summarized route, disable the automatic route summary function. Only when RIPv2 is configured, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

The range of the supernet route is wider than that of the classful network. Therefore, this command takes no effect on the supernet route.

Configuration Examples

The following example disables automatic route summary of RIPv2.

```
QTECH (config)# router rip QTECH (config-router)# version 2
QTECH (config-router)# no auto-summary
```

Related Commands

Command	Description
version	Defines the RIP software versions: v1 or v2. Both v1 and v2 are supported by default.

Platform Description

N/A

1.3. bdf all-interfaces

Use this command to enable all interfaces running RIP to use the BDF function. Use the **no** form of this command to restore the default setting.

bdf all-interfaces no bdf all-interfaces

Parameter Description

Parameter	Description
N/A	N/A

Defaults

BFD is not configured by default.

Command Mode

Routing process configuration mode

Usage Guide With the BFD function enabled on the RIP, one BFD session will be established for the RIP routing information source (the source address of the RIP route update packet). Once the BFD neighbor fails, the RIP routing information will be invalid directly and no longer join routing or forwarding.

You can also use the interface configuration mode command **ip rip bfd [disable]** to enable or disable the BFD function on the specified interface, which takes precedence over the command **bfd**

all-interfaces in the routing progress configuration mode.

Configuration Examples

N/A

Related Commands

Command	Description
route ip	Creates the RIP routing progress and enters the routing process configuration mode.
ip rip bfd [disable]	Configures a specified interface running RIP to enable or disable link detection using the BFD.

Platform Description

N/A

1.4. default-information originate

Use this command to generate a default route in the RIP process. Use the **no** form of this command to delete the generated default route.

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Enables RIP to generate the default route, no matter whether the default route exists or not.
metric <i>metric-value</i>	(Optional) The original metric value of the default route with the value range 1 to 15 of metric-value.
route-map <i>map-name</i>	(Optional) Name of the associated route-map. Route-map is not associated by default.

Defaults

No default route is generated by default.

The default metric value is 1.

Command Mode

Routing process configuration mode

Usage Guide B

By default, RIP will not advertise the default route if the default route exists in the routing table of the router. In this case, use the **default-information originate** command to notify the neighbor of the default route.

With the parameter **always** configured, no matter whether the default route exists in the RIP routing process or not, the default route will be advertised to the neighbor but is not shown in the local routing table. You can use the **show ip rip database** command to view the RIP routing information database to confirm whether the default route is generated.

Use the parameter **route-map** to control more about the default route advertised to RIP. For example, use the **set metric** command to set the metric value of the default route.

The route-map set metric rule takes precedence over the parameter metric value configuration of the default route. If the parameter metric is not configured, the default metric value is used by the default route.

If the default route can be generated in the RIP process by using this command, RIP will not learn the default route advertised from the neighbor.

For the default route generated by using the ip default-network command, the default-information originate command is required to add the default route to RIP.

Configuration Examples

Related

The following example generates a default route to the RIP routing table.

```
QTECH(config-router)# default-information originatealways
```

Commands

Command	Description
ip rip default-information	Notifies the default route through an interface.
redistribute	Redistributes the routes from other protocols to RIP.

Platform Description

N/A

1.5. default-metric

Use this command to define the default RIP metric value. Use the **no** form of this command to restore the default setting.

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
<i>metric-value</i>	Indicates the default metric value with the range from 1 to 16. If the metric value is greater than or equal to 16, the RGNOS regards the

	route unreachable.
--	--------------------

Defaults

The default is 1.

Command Mode

Routing process configuration mode

Usage Guide

This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric value cannot be converted due to the incompatibility of the metric calculation mechanisms for different protocols. During the conversion, therefore, it is required to redefine the metric values of redistributed routes in the RIP routing domain. If there is no clear definition of the metric value in redistributing a routing protocol process, the RIP uses the metric value defined with **default-metric**. If the metric value is defined, this value overwrites the metric value defined with default-metric. If this command is not configured, the default value of default-metric is 1.

Configuration Examples

The following example enables the RIP routing protocol to redistribute the routes learned by the OSPF routing protocol, whose initial RIP metric value is set to 3.

```
QTECH (config)# router rip
QTECH (config-router)# default-metric 3 QTECH (config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the routes from one routing
	domain to another routing domain.

Platform Description

N/A

1.6. distance



Use this command to set the management distance of the RIP route. Use the **no** form of this command to restore the default setting.

distance *distance* [*ip-address wildcard*]

no distance [*distance ip-address wildcard*]

Parameter Description

Parameter	Description
<i>distance</i>	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
<i>ip-address</i>	Indicates the prefix of the source IP address of the route.
<i>wildcard</i>	Defines the comparison bit of the IP address, where 0 means accurate matching and 1 means no comparison.

Defaults The default is 120.

Command Mode

Routing process configuration mode

Usage Guide

Use this command to set the management distance of the RIP route.

You can use this command to create several management distances with source address prefixes. When the source address of the RIP route is within the range specified by the prefixes, the corresponding management distance is applied; otherwise, the route uses the management distance configured by the RIP.

Configuration Examples

The following example sets the management distance of the RIP route to 160, and specifies the management distance of the route learned from 192.168.2.1 as 123.

```
QTECH(config)# router rip QTECH(config-router)# distance 160
QTECH(config-router)# distance 123 192.168.12.1 0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

1.7. distribute-list in

Use this command to control route update for route filtering. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } [**gateway** *prefix-list-name*] } **in** [*interface-type* *interface-number*]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] }

| [**gateway** *prefix-list-name*] } **in** [*interface-type* *interface-number*]

Parameter Description

Parameter	Description
<i>access-list-number</i> <i>name</i>	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
prefix <i>prefix-list-name</i>	Uses the prefix list to filter the routes.
gateway <i>prefix-list-name</i>	Uses the prefix list to filter the source of the routes.
<i>interface-type</i> <i>interface-number</i>	(Optional) Applies the distribution list only to a specified interface.

Defaults

The distribution list is not defined by default.

Command Mode

Routing process configuration mode

Usage Guide

To deny receiving some specified routes, you can process all the received route update packets by configuring the route distribute control list.

Without any interface specified, the system will process the route update packets received on all the interfaces.

Configuration Examples

The following example enables RIP to control the routes received from the Fastethernet 0/0, only permitting the routes starting with 172.16.

```
QTECH (config)# router rip
QTECH (config-router)# network 200.168.23.0
QTECH (config-router)# distribute-list 10 in fastethernet 0/0 QTECH (config-router)# no
auto-summary
QTECH (config-router)# access-list 10 permit 172.16.0.0 0.0.255.255
```

Related Commands

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.

1.8. distribute-list out

Use this command to control route update advertisement for filtering routes. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* | [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* | [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]]

Parameter Description

Parameter	Description
<i>access-list-number</i> <i>name</i>	Specifies the ACL.
prefix <i>prefix-list-</i>	Uses the prefix list to filter routes.



<i>name</i>	
<i>interface</i>	(Optional) Applies route update advertisement control to a specified interface in the distribution list.
bgp	(Optional) Applies route update advertisement control to only routes introduced from bgp in this distribution list.
connected	(Optional) Applies route update advertisement control to only connected routes in this distribution list.
isis [<i>area-tag</i>]	(Optional) Applies route update advertisement control to only routes introduced from ISIS in this distribution list. <i>area-tag</i> specifies an ISIS instance.
ospf <i>process-id</i>	(Optional) Applies route update advertisement control to only routes introduced from OSPF in this distribution list. <i>process-id</i> specifies an OSPF instance.
rip	(Optional) Applies route update advertisement control to only RIP routes in this distribution list.
static	(Optional) Applies route update advertisement control to only static routes in this distribution list.

Defaults

No route update advertisement is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

If this command relates to none of optional parameters, route update advertisement control applies to all interfaces. If this command relates to interface options, route update advertisement control applies to only the specified interface. If this command relates to

other route process parameters, route update advertisement control applies to only the specific route process.

Configuration Examples

The following example advertises only the 192.168.12.0/24 route.

```
QTECH (config)# router rip
QTECH (config-router)# network 200.4.4.0 QTECH (config-router)# network 192.168.12.0
```

```
QTECH (config-router)# distribute-list 10 out QTECH (config-router)# version 2
QTECH (config-router)#access-list 10 permit 192.168.12.0 0.0.0.255
```

Related Commands

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.
redistribute	Configures route redistribution.

Platform Description

N/A

1.9. enable mib-binding

Use this command to bind a MIB with a specified RIP instance. Use the **no** form of this command to restore the default setting

enable mib-binding no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the MIB is bound with the RIP instance of the default VRF.

Command Mode

Routing process configuration mode.

Usage Guide

As RIP MIB does not have RIP instance information, you can only operate only one RIP instance using SNMP. By default, RIP MIB is bound with the RIP instance of the default VRF. You can only operate this RIP instance. If you want to operate another RIP instance of a specified VRF through SNMP, you can use this command to bind the MIB with this instance.

Configuration Examples

The following example operates the RIP instance of a specified VRF, vpn1.

```
QTECH(config)# router rip
QTECH(config-router)# address-family ipv4 vrf vpn1 QTECH(config-router-af)# enable mib-binding
```

Related Commands

Command	Description
show ip rip	Displays the global configuration of RIP.

Description

1.10. exit-address-family

Use this command to exit the address family configuration mode
exit-address-family

Parameter Description

Parameter	Description
N/A	N/A



Defaults

N/A

Command **Mode** A

address family configuration mode

Usage Guide

Use this command to exit the address family configuration mode.

The abbreviation of this command is exit.

Configuration Examples

The following example enters or exits the address family configuration mode.

```
QTECH(config-router)# address-family ipv4 vrf vpn1
QTECH(config-router-af)# exit-address-family
```

Related Commands

Command	Description
address-family	Enters the address family configuration sub-mode.

Platform Description

N/A

1.11. fast-reroute

Use this command to enable the RIP FRR (Fast Reroute) function for the device. Use the **no** form of this command to restore the default setting.

fast-reroute route-map *route-map-name*

no fast-reroute

Parameter Description

Parameter	Description
-----------	-------------

<i>route-map-name</i>	Specifies the backup path through the route map.
-----------------------	--

Command Mode

Routing process configuration mode

Usage Guide

Use the **route-map** command to specify the backup path for the matched routes.

It is recommended to enable the BFD function when the RIP fast reroute function is enabled. BFD allows the device to detect the link fault faster, so as to reduce the interruption time. In the scenario where the port is up/down, it is recommended to configure **carrier-delay 0** in interface configuration mode to achieve the fastest switchover speed, reducing the interruption time.

Currently, the restrictions of the RIP FRR are as follows: Only one backup next hop is generated for each route. The backup next hop is not generated for the ECMP route.

Configuration Examples

The following example enables FRR for RIP instance 1 and associates route map *fast reroute*.

```
QTECH(config)# route-map fast-reroute match interface gigabitEthernet 0/2
set fast-reroute backup-interface GigabitEthernet 0/1 backup-nexthop 192.168.1.1
QTECH(config)# router rip
QTECH(config-router)# fast-reroute route-map fast-reroute
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.12. graceful-restart

Use this command to configure the RIP graceful restart (GR) function for a device. Use the **no** form of this command to restore the default configuration.

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter Description

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	(Optional) Configures the grace period.
<i>grace-period</i>	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The range is from 1 to 1,800. The unit is second.

Defaults

This function is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

The GR function is configured on the RIP instances. Different parameters can be configured for different RIP instances.

The GR period refers to the time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation.

The **graceful-restart grace-period** command enables users to modify GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If an improper value is configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the period needs to be changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the **timers basic** command.

During the RIP GR period, the network must be stable.

Configuration Examples

The following example enables the RIP GR function and configures the GR period parameters of the GR function.

```
QTECH(config)# router rip
QTECH(config-router)# graceful-restart grace-period 90
```

Related Commands

Command	Description
timers basic	Configures RIP timers.

Platform Description

N/A

1.13. ip rip authentication key-chain

Use this command to enable RIP authentication and specify the keychain used for RIP authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication key-chain *name-of-keychain*

no ip rip authentication key-chain

Parameter Description

Parameter	Description
<i>name-of-keychain</i>	Indicates the name of the keychain, which specifies the keychain used for RIP authentication.

Defaults

The keychain is not associated by default.

Command Mode

Interface configuration mode

Usage Guide

If the keychain is specified in the interface configuration, use the key chain global configuration command to define the keychain. Otherwise, RIP data packet authentication fails.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples

The following example enables RIP authentication on the fastEthernet 0/1 with the associated keychain ripchain.

```
QTECH (config)#interface fastEthernet 0/1
QTECH (config-if-FastEthernet 0/1)#ip rip authentication key-chain ripchain
```

```
QTECH(config)#key chain ripchain
QTECH(config-keychain)#key 1
QTECH(config-keychain-key)#key-string Hello
```

Meanwhile, use the **key chain** command to define this keychain in global configuration mode.

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication text-password	Enables RIP authentication, and sets the password string of RIP plaintext authentication. RIP data packet authentication is supported only by RIPv2.
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
key chain	Defines the keychain and enters keychain configuration mode.

Platform Description

N/A

1.14. ip rip authentication mode

Use this command to define the RIP authentication mode. Use the **no** form of this command to restore the default setting.

ip rip authentication mode { text | md5 }

no ip rip authentication mode

Parameter Description

Parameter	Description
text	Configures RIP authentication as plaintext authentication.
md5	Configures RIP authentication as MD5 authentication.

Defaults

It is plaintext authentication by default.

Command Mode

Interface configuration mode

Usage Guide

During the RIP authentication configuration process, the RIP authentication modes of all devices requiring exchange of RIP routing information must be the same. Otherwise, RIP packet exchange will fail.

If the plaintext authentication mode is adopted, but the password string of the plaintext authentication or the associated keychain is not configured, no authentication occurs. In the same way, if the MD5 authentication mode is adopted, but the associated keychain is not configured, no authentication occurs.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples

The following example configures the RIP authentication mode on the fastEthernet 0/1 as MD5.

```
QTECH (config)#interface fastEthernet 0/1
QTECH (config-if-FastEthernet 0/1)# ip rip authentication mode md5
```

Related Commands

Command	Description
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication of the RIP data packet.
ip rip authentication text-password	Enables the RIP authentication mode, and sets the password string of RIP plaintext authentication. Only RIPv2 supports authentication of the RIP data packet.
key chain	Defines the keychain and enters the keychain configuration mode

Platform Description

N/A

1.15. ip rip authentication text-password

Use this command to enable RIP authentication and set the password string of RIP plaintext

Parameter Description

authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication text-password [0 | 7] *password-string*

no ip rip authentication text-password

Parameter	Description
0	Specifies that the key is displayed as plaintext.

7	Specifies that the key is displayed as cipher text.
<i>password-string</i>	Indicates the password string of the plaintext authentication, in the length of 1-16 bytes.

Defaults

No password string of RIP plaintext authentication is configured by default.

Command Mode

Interface configuration mode

Usage Guide

This command works only in plaintext authentication mode.

To enable the RIP plaintext authentication function, use this command to configure the corresponding password string, or use the associated key chain to obtain the password string. The latter takes the precedence over the former one.

RIPv1 does not support RIP authentication but RIPv2 does.

Configuration Examples

The following example enables the RIP plaintext authentication on fastEthernet 0/1 and sets the password string to hello.

```
QTECH(config)#interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip rip authentication text-password hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication.

Platform Description

N/A

1.16. ip rip bfd

Use the `ip rip bfd [disable]` command to configure the specified interface running RIP to enable or disable link detection using the BFD. Use the `no` form of this command to restore the default setting. `ip rip bfd [disable]`

`no ip rip bfd`

Parameter Description

Parameter	Description
disable	Disables the specified interface running RIP and uses the BFD mechanism to perform link detection.

Defaults

Interfaces running RIP are not configured by default. The BFD configuration in RIP process configuration mode is a reference.

Command Mode

Interface configuration mode

Usage Guide

The priority of the interface is higher than that of the `bfd all-interfaces` command in process configuration mode.

You can use the `ip rip bfd` command to enable the BFD to perform link detection on the specified interface according to the actual environment or use the `bfd all-interfaces` command to configure all interfaces running RIP and enable the BFD to perform link detection. In addition, you can use the `ip rip bfd disable` command to disable the BFD detection function on the specified interface.

Configuration Examples

N/A

Related Commands

Command	Description
	Enables the RIP routing process and enters the

route ip	routing process configuration mode.
bdf all-interfaces	Configures all interfaces running RIP to use the BFD to perform link detection.

Platform Description

N/A

1.17. ip rip default-information

Use this command to advertise the default route through a RIP interface. Use the **no** form of this command to restore the default setting.

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

no ip rip default-information

Parameter Description

Parameter	Description
only	Notifies the default route rather than other routes.
originate	Notifies the default route and other routes.
metric <i>metric-value</i>	Specifies the metric value of the default route, in the range from 1 to 15.

Defaults

No default route is configured by default. The default metric value is 1.

Command Mode

Interface configuration mode

Usage Guide

After you configure this command on a specified interface, a default route is generated and notified through the interface. If the **ip rip default-information** command of the interface and the

default-information originate command of the RIP process are configured at the same time, only the default route of the interface is advertised.

RIP will no longer learn the default route notified by the neighbor if any interface is configured with the **ip rip default-information** command.

Configuration Examples

```
QTECH(config)#interface ethernet 0/1
QTECH(config-if-Ethernet 0/1)#ip rip default-information only
```

The following example creates a default route which is notified on ethernet0/1 only.

Related Commands

Command	Description
default-information originate	Generates a default route in the RIP process.

Platform Description

N/A

1.18. ip rip receive enable

Use this command to enable RIP to receive the RIP data package on a specified interface. Use the

no form of this command to restore the default setting.

ip rip receive enable

no ip rip receive enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

RIP packages can be received through the interface by default.

Command Mode

Interface configuration mode

Usage Guide

To prevent an interface from receiving RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to receive the RIP data package.

Configuration Examples

The following example prohibits receiving RIP data packages on fastEthernet 0/1.

```
QTECH (config)# interface fastEthernet 0/1
QTECH (config-if-FastEthernet 0/1)# no ip rip receive enable
```

Related Commands

Command	Description
ip rip send enable	Enables or disables the interface to send RIP data packages.
passive-interface	Configures a passive RIP interface.

Platform Description

N/A

1.19. ip rip receive version

Use this command to define the version of RIP packets received on an interface. Use the **no** form of this command to restore the default setting.

ip rip receive version [1] [2]

no ip rip receive version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults

The default behavior depends on the configuration with the version command.

Command Mode

Interface configuration mode

Usage Guide

This command overwrites the default configuration of the **version** command. It affects only RIP packet receiving through the interface and allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If the command is configured without parameters, data package receiving depends on the configuration of the version.

Configuration Examples

The following example enables receiving both RIPv1 and RIPv2 data packages.

```
QTECH (config)#interface fastEthernet 0/1
QTECH (config-if-FastEthernet 0/1)# ip rip receive version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interface.

Platform Description

N/A

1.20. ip rip send enable

Use this command to enable RIP to send a RIP data package on a specified interface. Use the **no**

form of this command to restore the default setting.

ip rip send enable no ip rip send enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

RIP packages can be sent through the interface by default.

Command Mode

Interface configuration mode

Usage Guide

To prevent an interface from sending RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to send the RIP data package.

Configuration Examples

The following example prohibits sending RIP data packages on fastEthernet 0/1.

```
QTECH (config)# interface fastEthernet 0/1
QTECH (config-if-FastEthernet 0/1)# no ip rip send enable
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on the interface.
passive-interface	Configures a passive RIP interface.

Platform Description

N/A

1.21. ip rip send supernet-routes

Use this command to enable RIP to send the supernet route on a specified interface. Use the no form

Parameter Description

of this command to disable this function.

ip rip send supernet-routes no ip rip send supernet-routes

Defaults

This function is enabled by default.

Parameter	Description
N/A	N/A

Command Mode

Interface configuration mode

Usage Guide When the RIPv1 router monitors a RIPv2 router response packet and if the supernet routing information is monitored, incorrect route information is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, you are advised to use the no form of this command on the RIPv2 router to disable advertising the supernet route on the corresponding interface. This command works only on interfaces configured with this command.

This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet route.

Configuration Examples

The following example disables sending RIP supernet routes on the fastEthernet 0/1 interface.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# no ip rip send supernet-routes
```

Related Commands

Command	Description
version	Defines the RIP version
ip rip send enable	Enables or disables sending the RIP package on the interface.

Platform Description

N/A

1.22. ip rip send version

Use this command to define the version of the RIP packets sent on the interface. Use the no form of this command to restore the default setting.

ip rip send version [1] [2]

no ip rip send version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults

The default behavior depends on the configuration with the version command.

Command Mode

Interface configuration mode

Usage Guide

This command overwrites the default configuration of the version command. It affects only RIP packet sending through the interface and allows RIPv1 and RIPv2

packages sent on the interface at the same time. If the command is configured without parameters, package receiving depends on the configuration of the version.

Configuration Examples

The following example enables sending both RIPv1 and RIPv2 packages on the fastEthernet 0/1 interface.

```
QTECH (config)# interface fastEthernet 0/1
QTECH (config-if-FastEthernet 0/1)# ip rip send version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interfaces.

Platform Description

N/A

1.23. ip rip split-horizon

Use this command to enable split horizon. Use the no form of this command to disable this function.

ip rip split-horizon [poisoned-reverse]

no ip rip split-horizon [poisoned-reverse]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables split horizon with poisoned reverse.

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode

Usage Guide

When multiple devices are connected to the IP broadcast network and run a distance vector routing protocol, the split horizon mechanism is required to prevent loop. The split horizon prevents the

device from advertising routing information from the interface that learns that information, which optimizes routing information exchange between multiple devices.

For non-broadcast multi-path access networks (such as frame relay and X.25), split horizon may cause some devices to be unable to learn all routing information. Split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for split horizon.

If the **poisoned-reverse** parameter is configured, split horizon with poisoned reverse is enabled. In this case, devices still advertise the route information through the interface from which the route information is learned. However, the metric value of the route information is set to unreachable.

The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, use the show ip rip command to judge. This function makes no influence on the neighbor defined with the **neighbor** command.

Configuration Examples

The following example disables the RIP split horizon function on the interface fastethernet 0/0.

```
uijie (config)# interface fastethernet 0/1
QTECH (config-if)# no ip rip split-horizon
```

Related Commands

Platform Description

Command	Description
neighbor (RIP)	Defines the IP address of the neighbor of RIP.
validate-update-source	Enables the source address authentication of the RIP route update message.

N/A

1.24. ip rip subvlan

Use this command to enable RIP on super VLANs. Use the **no** form of this command to restore the default setting.

ip rip subvlan [all | **vid**] no ip rip subvlan

Parameter Description

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults

The default setting takes effect only on super VLANs with RIP disabled.

Command Mode

Interface configuration mode

Usage Guide

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIPng multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIPng multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the RIPng function does not need to be enabled on a super VLAN. Therefore, the RIPng function is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration Examples

The following example sends the RIP multicast packets to sub VLAN 1024 of super VLAN 300.

```
QTECH(config)# interface vlan 300
```

```
QTECH(config-if-VLAN 300)# ip rip subvlan 1024
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.25. ip rip summary-address

Use this command to configure port-level convergence through an interface. Use the **no** form of this command to disable this function.

ip rip summary-address *ip-address ip-network-mask*

no ip rip summary-address *ip-address ip-network-mask*

Parameter Description

Parameter	Description
<i>ip-address</i>	Indicates the IP addresses to be converged.
<i>ip-network-mask</i>	Indicates the subnet mask of the specified IP address for route convergence.

Defaults

The RIP routes are automatically converged to the classful network edge by default.

Command Mode

Interface configuration mode

Usage Guide

The **ip rip summary-address** command converges an IP address or a subnet on a specified port.

RIP routes are automatically converged to the classful network edge.

The classful subnet can be configured through only port convergence.

The summary range configured by this command cannot be a super class network, that is, the configured mask length is greater than or equal to the natural mask length of the network.

Configuration Examples

The following example disables the automatic route convergence function of RIPv2. Interface convergence is configured so that fastEthernet 0/1 advertises the converged route 172.16.0.0/16.

```
QTECH (config)# interface fastEthernet 0/1
QTECH (config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0
QTECH (config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0 QTECH (config)#
router rip
QTECH (config-router)# network 172.16.0.0 QTECH (config-router)# version 2
QTECH (config-router)# no auto-summary
```

Related Commands

Command	Description
auto-summary	Enables the automatic convergence of RIP routes.

Platform Description

N/A

1.26. ip rip triggered

Use this command to enable triggered RIP based on links. Use the **no** form of this command to restore the default setting.

ip rip triggered

ip rip triggered retransmit-timer *timer* ip rip triggered retransmit-count *count* no ip rip triggered

no ip rip triggered retransmit-timer no ip rip triggered retransmit-count

Parameter Description

Parameter	Description
retransmit-timer <i>timer</i>	Configures the interval at which the Update Request and Update Response packets are retransmitted. The range is from 1 to 3,600. The unit is second. The default is five.

retransmit-count <i>count</i>	Configures the maximum times that the Update Request and Update Response packets are retransmitted. The range is from 1 to 3600. The default is 36.
---	---

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for demand-based links.

With the TRIP function enabled, RIP no longer sends route updates periodically and sends route updates to the WAN interface only if:

Update Request packets are received. RIP routing information is changed.

Interface state is changed. The router is started.

As periodical RIP update is disabled, the confirmation and retransmission mechanism is required to ensure that update packets are sent and received successfully over the WAN. The **retransmit-timer** and **retransmit-count** commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.

The function can be enabled in the case of the following conditions: a) The interface has only one neighbor. b) There are multiple neighbors but they interact information using unicast packets. You are advised to enable the function for link layer protocols such as PPP, frame relay, and X.25.

You are advised to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might be left.

Make sure that the function is enabled on all routers on the same link; otherwise the function will be invalid and the routing information cannot be exchanged correctly.

The function cannot be enabled at the same time with BFD and RIP functions.

To enable the function, make sure that the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.

If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source IP address verification function (validate-update-source)

is enabled.

Configuration Examples

The following example enables TRIP and sets the retransmission interval

1. RIP Commands

and maximum retransmission time to 10 seconds and 18 respectively for Update Request and Update Response packets.

```
QTECH(config)# interface fastEthernet 0/1 QTECH(config-if-
FastEthernet 0/1)# ip rip triggered
QTECH(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10
QTECH(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18
```

Related Commands

Command	Description
show ip rip database	Displays the summarized routing information of the RIP database.
show ip rip interface	Displays the RIP interface information.
ip rip split-horizon	Configures RIP split horizon.

Platform Description

N/A

1.27. ip rip v2-broadcast

Use this command to send RIPv2 packets in broadcast rather than multicast mode. Use the **no** form of this command to restore the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default behavior depends on the configuration of the version command.

Command Mode

configuration mode

Usage Guide

This command overwrites the default of the **version** command. This command affects only sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packages sent on the interface simultaneously. If this command is configured without parameters, package receiving depends on the version setting.

Configuration Examples

The following example sends RIPv2 packets in broadcast mode on the fastEthernet 0/1 interface.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# no ip rip split-horizon
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received and sent on the interface.

Platform Description

N/A

1.28. neighbor

Use this command to define the IP address of a RIP neighbor. Use the **no** form of this command to restore the default setting.

neighbor *ip-address*

no neighbor *ip-address*

Parameter Description

Parameter	Description
<i>ip-address</i>	Indicates the IP address of the neighbor. The IP address must be that of the network connected to the local device.

Defaults

The neighbor is not defined by default.

Command Mode

Routing process configuration mode

Usage Guide

By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 uses the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, use the **passive-interface** command to configure related interfaces as passive interfaces and then define only some neighbors who can receive the routing information. This command has no impact on the receiving of RIP information. The passive interface is configured. No request packet is sent after the interface is enabled.

Configuration Examples

The following example creates a VRF with the name of vpn1 and creates its RIP instance.

```
QTECH(config)# router rip
QTECH(config-router)# passive-interface default
QTECH(config-router)# neighbor 192.168.1.2
```

Related Commands

Command	Description
passive-interface	Configures the interface as a passive interface.

Platform Description

N/A

1.29. network

Use this command to define the list of networks to be advertised in the RIP routing process. Use the

no form of this command to delete the defined network.

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter Description

Parameter	Description
<i>network-number</i>	Indicates the network number of the directly-connected network. The network number is a natural one. All interfaces whose IP addresses belong to that natural network can send/receive RIP packages.
<i>wildcard</i>	Defines the IP address comparing bit: 0 refers to accurate matching, and 1 refers to no comparison.

Defaults

N/A

Command Mode

Routing process configuration mode

Usage Guide The *network-number* and *wildcard* parameters can be configured simultaneously to enable the IP address of the interface within the IP address range to join RIP running.

Without the *wildcard* parameter, OS make the interface IP address within the classful address range join the RIP running.

Only when the IP address of an interface is in the network list defined by RIP, RIP route update packets can be received and sent on the interface.

Configuration Examples

The following example defines two network numbers associated with RIP and allows the interface IP address between 192.168.12.0/24 and 172.16.0.0/24 to join RIP running.

```
QTECH (config)# router rip
QTECH (config-router)# network 192.168.12.0
QTECH (config-router)# network 172.16.0.0 0.0.0.255
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.30. offset-list

Use this command to increase the metric value of received or sent RIP routes. Use the no form of this command to restore the default setting.

offset-list { access-list-number | name } { in | out } offset [interface-type interface-number]

no offset-list { access-list-number | name { in | out } offset [interface-type interface-number]

Parameter Description

Parameter	Description
<i>access-list-number</i> <i>name</i>	Specifies the ACL.
<i>in</i>	Modifies the metric of the received routes using the ACL.
<i>out</i>	Modifies the metric of the sent routes using the ACL.
<i>offset</i>	Indicates the offset of changed metric values. The value is in the range from 0 to16.
<i>interface-type</i>	Applies the ACL to a specified interface.
<i>interface-number</i>	Specifies the interface number.

Defaults

No offset is specified by default.

Command Mode

Routing process configuration mode

Usage Guide

If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

Configuration Examples

Related Commands

Platform Description

The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7. `QTECH (config-router)# offset-list 7 out 7` The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastethernet 0/1.

```
QTECH (config-router)# offset-list 8 in 7 fastethernet0/1
```

Command	Description
N/A	N/A

N/A

1.31. output-delay

Use this command to modify the delay to send RIP update packets. Use the **no** form of this command to restore the default setting.

output-delay *delay*

no output-delay

Parameter Description

Parameter	Description
<i>delay</i>	Sets the delay to send RIP update packets, in the range from 8 to 50 in the unit of milliseconds.

Defaults

No sending delay is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible.

However, when a high-speed device sends a large number of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Configuration Examples

The following example sets the delay to send RIP update packets to 30 milliseconds.

```
QTECH(config)# router rip
QTECH(config-router)# output-delay 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.32. passive-interface

Use this command to disable the function of sending update packets on an interface. Use the **no** form of this command to restore the default setting.

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description

Parameter	Description
default	Sets all interfaces to the passive interfaces.
<i>interface-type interface-num</i>	Indicates the interface type and number.

Defaults

Interfaces are set to the non passive interfaces by default.

Command Mode

Routing process configuration mode

Usage Guide

The **passive-interface default** command sets all interfaces to the passive interfaces. You can use

no passive-interface *interface-type interface-num* command to set specified interfaces as non-passive interfaces.

After you set an interface to the passive interface, RIP route update packets will no longer be sent but

can be received through the interface. In this case, route update packets can be sent to a specified neighbor through the interfaces by using the **neighbor** command. You can use the **ip rip send enable** and **ip rip receive enable** commands to control whether route update packets can be sent or received through the interface.

Configuration Examples

The following example sets all interfaces to the passive interfaces and then sets ethernet0/1 to the non-passive interface.

```
QTECH(config-router)# passive-interface default
QTECH(config-router)# no passive-interface gigabitEthernet 0/1
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on the interface.
ip rip send enable	Enables or disables sending RIP packets on the interface.

Platform Description

N/A

1.33. redistribute

Use this command to redistribute external routes in route configuration mode. Use the **no** form of this command to restore the default setting.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [{ **level-1** | **level-1-2** |

level-2 }] [**match** { **internal** | **external** [**1|2**] | **nssa-external** [**1|2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [{ **level-1** | **level-1-2** |

| **level-2** }] [**match** { **internal** | **external** [**1|2**] | **nssa-external** [**1|2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]

Parameter Description

Parameter	Description
bgp	Is redistributed from bgp.
connected	Is redistributed from a connected route.
isis area-tag	Is redistributed from ISIS and specifies an ISIS instance through area-tag.
ospf process-id	Is redistributed from OSPF and specifies an OSPF instance through process-id. The value is in the range from 1 to 65535.
static	Is redistributed from static routes.
level-1 level-1-2 level-2	Is used when ISIS route redistribution is configured and specifies a route with a specific level for redistribution.
match	Is used when OSPF route redistribution is configured and filters a
	route with a specific level for redistribution.

metric <i>metric-value</i>	Sets the metric value of the redistributed route and specifies the metric value by using the metric-value parameter. The value is in the range from 1 to 16.
route-map <i>route-map-name</i>	Sets the redistribution filtering rule.

Defaults By default:

All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF.

The routes of Level-2 sub-types of the instance are redistributed when you configure ISIS redistribution.

All the routes of the protocol are redistributed for other routing protocols. The metric of the redistributed routes is 1 by default.

The route-map is not associated.

Command Mode

Routing process configuration mode

Usage Guide

This command is executed to redistribute external routes to RIP.

It is unnecessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. For RIP, the metric value is calculated based on hop counts; for OSPF, the metric value is calculated based on bandwidths. Therefore, their metrics are not comparable. However, a symbolic metric value must be set for route redistribution. Otherwise, route redistribution will fail.

When you configure ISIS route redistribution without the level parameter, only level-2 routes are redistributed by default. If the redistribution configuration is initialized with the level parameter, then all routes with level configured are redistributed. When the configuration is saved and level 1 and level 2 are configured at the same time, level 1 and level 2 are combined into the level-1-2 parameter to be saved.

When you configure redistribution of OSPF routes without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The no form of this command restores the setting to the default value.

The rule of configuring the no form of the redistribute command is as follows:

If the no form of this command specifies certain parameters, the parameters must be restored to the default configuration.

If the **no** form of this command does not specify any parameter, the command must be deleted. Assume that the following configurations are available.

```
redistribute isis 112 level-2
```

You can use the `no redistribute isis 112 level-2` command to modify the configuration.

According to the preceding rule, this command only restores the level-2 parameter to the default value. However, level-2 is also the default parameter value. Therefore, the configuration is still be saved as `redistribute isis 112 level-2` after you use the `no` form of this command.

To delete this command, use the following command:

```
no redistribute isis 112
```

The `redistribute` command cannot redistribute the default route of other protocol to the RIP process. To this end, use the **default-information originate** command.

Configuration Examples

Related Commands

Platform Description

The following example redistributes static routes to RIP.

```
QTECH(config-router)# redistribute static
```

Command	Description
default-metric <i>metric</i>	Sets the default metric of the route to be redistributed.
default-information originate	Generates the default route in the RIP process.

N/A

1.34. router rip

Use this command to create the RIP routing process and enter the routing process configuration mode. Use the **no** form of this command to restore the default setting.

```
router rip no router rip
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No RIP process is running by default.

Command Mode

Global configuration mode

Usage Guide

One RIP routing process must be defined with one network number. If a dynamic routing protocol runs on asynchronous lines, configure the async default routing command on the asynchronous interface.

Configuration Examples

The following example creates the RIP routing process and enters the routing process configuration mode.

```
QTECH (config)# router rip
QTECH(config-router)#
```

Related Commands

Command	Description
network (RIP)	Defines the network number of the RIP process.

Platform Description

N/A

1.35. show ip rip

Use this command to display the RIP process information.


```
show ip rip [ vrf vrf-name ]
```

Parameter Description

Parameter	Description
vrf vrf-name	(Optional) Displays the RIP information with the specified VRF.

Defaults

N/A

Command Mode

Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide

It is used to display the three timers, routing distribution status, routing re-distribution status, interface RIP version, RIP interface and network range, metric, and distance of the RIP process quickly. If the VRF is specified, the name of VRF and VRF ID are displayed.

Configuration Examples

The following example displays the basic information of the RIP process such as the update time and management distance.

Current Restart remaining time 16 secs The following example specifies the VRF and displays the corresponding basic information of RIP instance.

```
QTECH#show ip rip Routing Protocol is "rip"
  Sending updates every 10 seconds,
  Invalid after 20 seconds, flushed after 10 seconds Outgoing update filter list for all
  interface is: not set Incoming update filter list for all interface is: not set Default
  redistribution metric is 2
  Redistributing: connected
  Default version control: send version 2, receive version 2
```

```
QTECH(config-router)# sh ip rip vrf 1 VRF 1 VRF-id:1
Routing Protocol is "rip"
  Interface          Send  Recv
  FastEthernet 0/1    2    2
```

1. RIP Commands

66

```
FastEthernet 0/2          2      2
192.168.26.0 255.255.255.0
192.168.64.0 255.255.255.0
Distance: (default is 50)
Graceful-restart enabled Restart grace period 60 secs
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.36. show ip rip database

Use this command to display the route summary information in the RIP routing database.

show ip rip database [**vrf** *vrf-name*] [*network-number network-mask*] [**count**]

Parameter Description

Parameter	Description
vrf <i>vrf-name</i>	(Optional) Displays the RIP routing information of specified VRF.
<i>network-number</i>	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
<i>network-mask</i>	Indicates the subnet mask. It must be specified if the network number is specified.
count	(Optional) Displays the abstract of the route statistics in the RIP database.

CommandMode

Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide

Only when the related sub-routes are converged, the converged address entries appear in the RIP

routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.

Configuration

The following example displays all converged address entries in the RIP routing database.

```
Examples    QTECH# show ip rip database
192.168.1.0/24 auto-summary
192.168.1.0/30 directly connected, Loopback 3
192.168.1.8/30 directly connected, FastEthernet 0/1
192.168.121.0/2 auto-summary
4
192.168.121.0/2 redistributed
4
[1] via 192.168.2.22, FastEthernet 0/2 192.168.122.0/24 auto-summary
192.168.122.0/24
[1] via 192.168.4.22, Serial 0/1 00:28 permanent
```

The following example displays the converged address entries related with 192.168.121.0/24 in the RIP routing database.

```
QTECH# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24 redistributed
[1] via 192.168.2.22, FastEthernet 0/1
```

Related Commands

Platform Description

The following example displays the statistical information summary of various routes in the RIP routing database.

```
QTECH# show ip rip database count
```

	A	Vali	Invalid
	1	d	
	1		
database	5	5	0
auto-summary	5	5	0
connected	1	1	0
rip	4	4	0

Command	Description
show ip rip	Displays the information of the currently-running routing protocol process.

N/A

1.37. show ip rip external

Use this command to display the information of the external routes redistributed by the RIP protocol. *show ip rip external [bgp | connected | isis [process-id] | ospf process-id | static] [vrf vrf-name]*

Parameter Description

Parameter	Description
bgp	Displays redistributed BGP routes.
connected	Displays redistributed directly-connected routes.
isis process-id	Displays redistributed ISIS routes. The process-id parameter indicates ISIS process ID.
ospf process-id	Displays redistributed OSPF routes. The process-id parameter indicates OSPF process ID. The range is from 1 to 65535.
static	Displays redistributed static routes.
vrf vrf-name	Displays the RIP external route of the specified VRF (optional).

Defaults

N/A

Command Mode

Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Configuration Examples

```
QTECH# show ip rip external Protocol connected
route: [connected] 192.100.3.0/24 metric=0
      nhop=0.0.0.0, if=2
[connected] 192.101.1.0/24 metric=0 nhop=0.0.0.0,
      if=3
Protocol static route: [static] 10.1.1.1/32
metric=0
      nhop=0.0.0.0, if=4096 [static]
10.1.2.1/32 metric=0
      nhop=0.0.0.0, if=4096 Protocol ospf 1
route: [ospf] 1.1.1.1/32 metric=2
      nhop=192.100.3.2, if=2
[ospf] 90.1.1.1/32 metric=2
      nhop=192.100.3.2, if=2
```

The following example displays direct routes redistributed by the RIP process.

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.
ip vrf	Creates a VRF.

Platform Description

N/A

1.38. show ip rip interface

Use this command to display the RIP interface information.

show ip rip interface [vrf vrf-name] [interface-type interface-number]

Parameter Description

Parameter	Description
-----------	-------------

1. RIP Commands

vrf <i>vrf-name</i>	Displays the RIP interface of specified VRF (optional).
[<i>interface-type</i> <i>interface-number</i>]	Displays the specified interface type and interface number (optional).

Defaults

N/A

Command Mode

Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide

This command is used to display the information about RIP interfaces. If no RIP interface exists, no information is displayed.

Configuration Examples

The following example displays the RIP interface information.

2.2.2.57/24, next update due in 16 seconds

```
QTECH# show ip rip interface
FastEthernet 0/1 is up, line protocol is up Routing
Protocol: RIP
Receive RIPv2 packets only Send RIPv2
packets only Recv RIP packet total: 0 Send
RIP packet total: 3 Passive interface:
Disabled
Split Horizon with Poisoned Reverse: Enabled Triggered RIP
Enabled:
Retransmit-timer: 5, Retransmit-count: 36 V2 Broadcast:
Disabled
Multicast registe: Registered Interface
Summary Rip:
QTECH#show ip rip interface
Serial 0/1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv1 and RIPv2 packets
Send RIPv1 packets only
Receive RIP packet: Enabled
Send RIP packet: Enabled
Send RIP supernet routes: Enabled
Recv RIP packet total: 0
Send RIP packet total: 3
```

```

Passive interface: Disabled Split Horizon:
Enabled Triggered RIP Disabled
BFD: Enabled
V2 Broadcast: Disabled
Multicast registe: Registered
Interface Summary Rip:
    Not Configured
IP interface address:
    2.2.2.111/24, next update due in 14 seconds

```

If the BFD has been configured for RIP, the BFD information is also displayed.

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.

Platform Description

N/A

1.39. show ip rip peer

Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP neighbor information.

```
show ip rip peer [ ip-address ] [ vrf vrf-name ]
```

Parameter Description

Parameter	Description
<i>ip-address</i>	(Optional) Displays the IP address of a specified RIP neighbor.
vrf vrf-name	(Optional) Displays the RIP interface of a specified VRF.

Defaults

N/A

Command Mode

Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide

This command is used to display the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.

Configuration Examples

The following example displays the RIP neighbor information.

```
QTECH# show ip rip peer Peer
192.168.3.2:
  Local address: 192.168.3.1
  Input interface: GigabitEthernet 0/2 Peer version:
  RIPv1
  Received bad packets: 3
  Received bad routes: 0 BFD session
  state up
```

Related Commands

Command	Description
show ip rip	Displays the information of the routing protocol process that is running.

Platform Description

N/A

1.40. timers basic

Use this command to adjust the RIP clock. Use the no form of this command to restore the default setting.

timers basic update invalid flush

no timers basic

Parameter Description

Parameter	Description
-----------	-------------

update	Indicates the route update time in seconds. The update keyword defines the period at which the device sends route update packets. Each time an update packet is received, the "Invalid" and "Flush" clocks are reset. By default, a route update packet is sent every 30 seconds.
invalid	Indicates the route invalid time in seconds, starting from the last valid update packet. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update packet is received within the route invalid period, the related
	route becomes invalid and enters into the "invalid" state. If an update packet is received within the period, the clock resets. By default, the Invalid time is 180 seconds.
flush	Indicates the route flushing time in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush time is 120 seconds.

Defaults

By default, the update time is 30 seconds, the invalid time is 180 seconds, and the flushing time is 120 seconds.

Command Mode

Routing process configuration mode

Usage Guide

Adjusting the above clocks may speed up routing protocol convergence and fault recovery. Devices connected to the same network must have consistent RIP clock values. Adjustment of RIP clocks is not recommended unless otherwise specified.

To check the current RIP clock parameters, use the show ip rip command.

If you set the clock to a small value on low-speed links, some risks will be caused because numerous update packets may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2 Mbit/s to reduce the convergence time of routes.

Configuration Examples

The following example enables the RIP update packets that are sent every 10 seconds. If no update packet is received within 30 seconds, related routes become invalid and enter the invalid status.

When another 90s elapses, they will be cleared.

```
QTECH (config)# router rip
QTECH (config-router)# timers basic 10 30 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.41. validate-update-source

Use this command to validate the source address of the received RIP route update packet. Use the

no form of the command to disable this function.

validate-update-source

no validate-update-source

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

You can validate the source address of the RIP route update packet. The validation aims to ensure that the RIP routing process receives only the route update packets from the same IP subnet neighbor.

Disabling split horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the **validate-update-source** command in routing process configuration mode.

In addition, for the ip unnumbered interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the command **validate-update-source**.

Configuration Examples

The following example disables verification of the source IP address of the update packet.

```
QTECH (config)# router rip
QTECH (config-router)# no validate-update-source
```

Related Commands

Command	Description
ip split-horizon	Enables split horizon.
ip unnumbered	Defines the IP unnumbered interface.
neighbor (RIP)	Defines the IP address of a RIP neighbor.

Platform Description

N/A

1.42. version

Use this command to define the RIP version of a device. Use the no form of this command to restore the default setting.

version { 1 | 2 }

no version

Parameter	Description
-----------	-------------

1	Defines the RIP version 1.
2	Defines the RIP version 2.

Defaults

The route update packets of RIPv1 are received by default, but only the RIPv1 route update packets are sent.

Command Mode

Routing process configuration mode

Usage Guide

This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the `ip rip receive version` and `ip rip send version` commands.

Configuration Examples

The following example configures the RIP version as version 2.

```
QTECH (config)# router rip
QTECH (config-router)# version 2
```

Related Commands

Command	Description
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
show ip rip	Displays RIP information.

Platform Description

N/A

2. OSPFV2 COMMANDS

2.1. area

Use this command to configure the specified OSPF area. Use the **no** form of this command to restore the default setting.

area *area-id*

no area *area-id*

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the OSPF area. The value can be a decimal integer or an IP address.

Defaults

No OSPF area is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

Use the no form of this command to remove the specified OSPF area and its configuration, including the area-based **area authentication**, **area default-cost**, **area filter-list**, and **area nssa** commands.

Do not remove the OSPF area configuration under the following conditions:

Virtual links exist in the backbone area. The virtual links must be removed at first.

The corresponding network area command exists in any area. All network segment commands added to an area must be removed at first.

Configuration Examples

The following example removes the configuration of OSPF area 2.

```
QTECH(config)# router ospf 2
QTECH(config-router)# no area 2
```

Command	Description
network area	Defines the interface where OSPF runs and the belonging area of the interface.

2.2. area authentication

Use this command to enable OSPF area authentication. Use the **no** form of this command to restore the default setting.

area area-id authentication [message-digest]

no area area-id authentication

Parameter Description

Parameter	Description
<i>area-id</i>	Specifies ID of the area enabled with OSPF. The value can be a decimal integer or an IP address.
message-digest	(Optional) Enables MD5 (message digest 5) authentication mode.

Defaults

No authentication is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

The software supports three authentication types:

1) 0, no authentication. The authentication type in the OSPF packet is 0 when this command is not executed to enable OSPF authentication. 2) 1, plain text authentication mode. When this command is configured, the message-digest option is not used. 3) 2, MD5 authentication mode. When this command is configured, the message-digest option is used.

All devices in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication password must be configured on an interface connecting neighbors. You can use the **ip ospf authentication-key** command to configure the plain

text authentication password, and the **ip ospf message-digest-key** command to configure the MD5 authentication password in interface configuration mode.

Configuration Examples

The following example uses MD5 authentication and the authentication password backbone in area 0 (backbone area) of the OSPF routing process.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 192.168.12.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf message-digest-key 1 md5 backbone
QTECH(config)# router ospf 1
QTECH(config-router)# network 192.168.12.0 0.0.0.255 area 0
QTECH(config-router)# area 0 authentication message-digest
```

Related Commands

Command	Description
ip ospf authentication-key	Defines the OSPF plain text authentication password.
ip ospf message-digest-key	Defines the OSPF MD5 authentication password.
area virtual-link	Defines a virtual link.

Platform Description

N/A

2.3. area default-cost

Use this command to define the cost (OSPF metric) of the default aggregate route advertised to the stub area or not-so-stubby area (NSSA) in routing process configuration mode. Use the **no** form of this command to restore the default setting.

area *area-id* **default-cost** *cost*

no **area** *area-id* **default-cost**

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the stub area or NSSA

<i>cost</i>	Cost of the default aggregate route advertised to the stub area or NSSA. The range is from 0 to 16777215.
-------------	--

Defaults

The default is 1.

Command Mode

Routing process configuration mode

Usage Guide

This command takes effect only on the Area Border Router (ABR) of the stub area or the ABR/Autonomous System Border Router (ASBR) of the NSSA.

The ABR can advertise a Link State Advertisement (LSA) indicating the default route in the stub area. The ABR/ASBR can advertise an LSA indicating the default route in the NSSA. You can use the **area default-cost** command to modify the LSA cost.

Configuration Examples

The following example sets the cost of the default aggregate route to 50.

```
QTECH(config)# router ospf 1
QTECH(config-router)# network 172.16.0.0 0.0.255.255 area 0
QTECH(config-router)# network 192.168.12.0 0.0.0.255 area 1
QTECH(config-router)# area 1 stub
QTECH(config-router)# area 1 default-cost 50
```

Related Commands

Command	Description
area stub	Sets an OSPF area as a stub area.
area nssa	Sets an OSPF area as an NSSA.

Platform Description

N/A

2.4. area filter-list

Use this command to filter the inter-area routes on the ABR. Use the **no** form of this command to restore the default setting.

area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } { **in** | **out** }

no area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } { **in** | **out** }

Parameter Description

Parameter	Description
<i>area-id</i>	Area ID
<i>acl-name</i>	Name of an Access Control List (ACL)
<i>prefix-name</i>	Prefix-list name
in out	Applies the ACL rule to the routes incoming/outgoing the area.

Defaults

No filtering is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

This command can be configured only on an ABR.

You can use this command when it is required to filter the inter-area routes on the ABR.

Configuration Examples

The following example sets area 1 to learn only the inter-area routes of 172.22.0.0/8.

```
QTECH# configure terminal
QTECH(config)# access-list 1 permit 172.22.0.0 0.255.255.255 QTECH(config)#
router ospf 100
QTECH(config-router)# area 1 filter-list access 1 in
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.5. area nssa

Use this command to set an OSPF area as an NSSA in routing process configuration mode. Use the

no form of this command to delete the NSSA or the NSSA configuration.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]

Parameter Description

Parameter	Description
<i>area-id</i>	NSSAID
no-redistribution	Imports the routing information to a common area other than the NSSA for the NSSA ABR.
default-information originate	Generates and imports the default Type 7 LSA to the NSSA. This option takes effect only on the NSSA ABR or ASBR.
metric <i>value</i>	Sets the metric of the generated default LSA. The range is from 0 to 16777214. The default value is 1.
metric-type <i>type</i>	Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
no-summary	Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
translator	Configures the translator for the NSSA ABR.
stability-interval <i>seconds</i>	Configures the stability interval in seconds for the NSSA ABR that functions as a translator to

	change to a non-translator. The range is from 0 to 2147483647. The default value is 40.
always	Configures that an NSSA ABR always functions as a translator. The NSSA ABR is the backup translator by default.

no area *area-id* nssa [no-redistribution] [default-information-originate [metric *value*] [metric-type *type*]] [no-summary] [translator [stability-interval | always]]

Defaults

No NSSA is defined by default.

Command Mode

Routing process configuration mode

Usage Guide

The default-information-originate parameter is used to generate the default Type-7 LSA. However, on the NSSA ABR, the default Type-7 LSA will always be generated; On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table.

The no-redistribution parameter prevents the OSPF from advertising the external routes imported with the redistribute command to the NSSA on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR.

To reduce the number of LSAs sent to the NSSA, you can configure the no-summary parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSAs) to the NSSA. In addition, you can use the area default-cost command on the NSSA ABR to configure the cost of the default route advertised to the NSSA. By default, this cost is 1.

If an NSSA has multiple ABRs, the ABR with the greatest ID is selected as the Type-7 or Type-5 translator. To configure that an NSSA ABR always functions as a translator, you can use the translator always parameter. If the translator role of an ABR is taken away by another ABR, the ABR still possesses the conversion capability within stability-interval. If the ABR fails to take back its translator role when stability-interval expires, the LSA that changes from Type-7 to Type-5 will be removed from the autonomous domain.

To avoid route loops, Type-5 LSAs generated from Type-7 convergence will be eliminated immediately after the current device stopped serving as a translator, with no need to wait until the stability-interval expires.

In a same NSSA, you are recommended to configure the **translator always** parameter on only one ABR.

Configuration Examples

The following example sets area 1 as an NSSA on all routers of the area.

```
QTECH(config)#router ospf1
QTECH(config-router)#network 172.16.0.0 0.0.255.255 area0
QTECH (config-router)#network 192.168.12.0 0.0.0.255 area 1 QTECH(config-
router)# area1nssa
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric) of the default aggregate route advertised to the NSSA.

Platform Description

N/A

2.6. area range

Use this command to configure inter-area route aggregation for OSPF. Use the no form of this command to delete route aggregation. Use the no form with the cost parameter to restore the default metric of the aggregate route, but not delete route aggregation.

area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area-id* **range** *ip-address net-mask* [**cost**]

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the area where the aggregate route is injected into. The value can be a decimal integer or an IP address.
<i>ip address net-mask</i>	Network segment whose routes are to be aggregated
advertise not-advertise	Whether to advertise the aggregate route
cost <i>cost</i>	Sets the priority of the interface. The range is from 0 to 16777215.

Defaults

No inter-area route aggregation is configured by default. The configured aggregation range is advertised by default.

The default metric of the aggregate route depends on whether the device is compatible with RFC1583. If yes, the default metric is the smallest cost of the aggregate route. If no, the default metric is the largest cost of the aggregate route.

Command Mode

Routing process configuration mode

Usage Guide

This command takes effect only on the ABR to aggregate multiple routes of an area into a route and advertise it to other areas. Route combination occurs only on the border of an area. The devices inside an area see the specific routing information, but the devices outside the area see only one aggregate route. The advertise and not-advertise options can set whether to advertise the aggregate route for filtering and masking. The aggregate route is advertised by default.

You can use the cost option to set the metric of the aggregate route.

You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing area. This improves the network forwarding performance, especially in large networks.

The area range of route aggregation is determined according to the longest match when multiple aggregate routes with direct inclusion relationships are configured.

Configuration Examples

The following example aggregate the routes of area 1 into a route 172.16.16.0/20.

```
QTECH(config)#router ospf 1
QTECH(config-router)#network 172.16.0.0 0.0.15.255area0
QTECH((config-router)#network 172.16.17.0 0.0.15.255area1
QTECH(config-router)#area1range 172.16.16.0 255.255.240.0
```

Related Commands

Command	Description
discard-route	Enables a discarded route to be added to a routing table.
summary-address	Configures the OSPF external route aggregation.

Platform Description

N/A

2.7. area stub

Use this command to set an OSPF area as a stub area or full stub area. Use the no form of this command to restore the default setting.

```
area area-id stub [ no-summary ]
```

```
no area area-id stub [ no-summary ]
```

Parameter Description

Parameter	Description
<i>area-id</i>	Stub area ID
no-summary	(Optional) Prevents the ABR from advertising the network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.

Defaults

No stub area is defined by default.

Command Mode

Routing process configuration mode

Usage Guide

All devices in the OSPF stub area must be configured with the area stub command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. For the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR.

To configure a full stub area, use the area stub command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR.

Two commands can configure an OSPF area as a stub area: the area stub and area default-cost commands. All devices connected to the stub area must be configured with the area stub command, but the area default-cost command can be executed only on the ABR. The area default-cost command defines the initial cost (metric) of the internal default route.

Configuration Examples

The following example sets area 1 as the stub area on all devices in area 1.

```
QTECH(config)# router ospf1
```

```
QTECH(config-router)# network 172.16.0.0 0.0.255.255 area 0
```

```
QTECH (config-router)# network 192.168.12.0 0.0.0.255 area 1
QTECH(config-router)# area 1 stub
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric value) of the default aggregate route advertised to the stub area.

Platform Description

N/A

2.8. area virtual-link

Use this command to define the OSPF virtual link in routing process configuration mode. Use the **no**

form of this command to restore the default setting.

area *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**dead-interval**

[*seconds* | **minimal hello-multiplier** *multiplier*]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [[**authentication-key** [**0|7**] *key*] | [**message-digest-key** *key-id* **md5** [**0|7**] *key*]]

no area *area-id* **virtual-link** *router-id* [**authentication**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [[**authentication-key**] | [**message-digest-key** *key-id*]]

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the OSPF transition area. The value can be a decimal integer or an IP address.
<i>router-id</i>	ID of the router neighboring to the virtual link. It can be viewed with the <code>show ip ospf</code> command.

dead-interval <i>seconds</i>	(Optional) Defines the time to declare neighbor loss in seconds. The range is 0 to 2147483647. This value must be consistent with that of the neighbor.
minimal	Enables the Fast Hello function and sets the death clock to 1 second.
hello-multiplier	Multiplies dead-interval with hello-interval in the Fast-Hello function.
<i>multiplier</i>	Specifies the number of Hello packets that are sent every second in the Fast Hello function. The range is from 3 to 20.
hello-interval <i>seconds</i>	(Optional) Defines the interval at which the HELLO packet is sent by the OSPF to the virtual link in seconds. The range is from 1 to 65535. This value must be consistent with that of the neighbor.
retransmit-interval <i>seconds</i>	(Optional) OSPF LSA retransmission interval in seconds. The range is from 0 to 65535. The parameter setting must consider the round-trip time of packets on the link.
transmit-delay <i>seconds</i>	(Optional) OSPF LSA transmission delay in seconds. The range is from 0 to 65535. This value adds the LSA keep alive period. When the LSA keep alive period reaches a threshold, the LSA will be refreshed.
authentication-key <i>[0 7]key</i>	(Optional) Defines the OSPF plain text authentication key. The plain text authentication key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.

message-digest-key <i>key-id md5 [0 7] key</i>	(Optional) Defines the OSPF MD5 authentication key and key ID. The MD5 authentication key ID and key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
authentication	Sets the authentication type to plain text.
message-digest	Sets the authentication type to MD5.
null	Sets the authentication type to no authentication.

Defaults

The following are the default values:

dead-interval: 40seconds hello-interval: 10seconds retransmit-interval: 5seconds transmit-delay: 1second authentication: null

The Fast Hello function is disabled by default. The other parameters do not have default values.

Command Mode

Routing process configuration mode

Usage Guide

A virtual link can connect an area to the backbone area, or another non-backbone area. In the OSPF routing domain, all areas must connect to the backbone area. If an area disconnects from the backbone area, a virtual link to the backbone area is required. Otherwise, the network communication will become abnormal. The virtual link is created between two ABRs. The area that belongs to both ABRs is called the transition area, which can never be a stub area or NSSA.

The router-id parameter indicates the ID of OSPF neighbor router and can be displayed with the show ip ospf neighbor command. You can configure the loopback address as the router ID.

The area virtual-link command defines only the authentication key for a virtual link. You can use the area authentication command to enable the OSPF packet authentication in areas connected over the virtual link in routing process configuration mode.

OSPF supports the Fast Hello function.

If the Fast Hello function is enabled, the OSPF can discover neighbors and detects invalid neighbors quickly. You can enable the OSPF Fast Hello function by specifying the keywords minimal and

hello-multiplier, and the multiplier parameter. You can set the death clock to 1 second in minimal and hello-multiplier to a value equal to or greater than 2. In this case, the Hello packet sending interval is less than 1 second.

The hello-interval field of a Hello packet received by a virtual link is omitted if the Fast Hello function is enabled on the virtual link and the hello-interval field is set to 0 for Hello packets advertised from the virtual link.

No matter the Fast Hello function is enabled or not, the values of dead-interval must be consistent on both ends of a virtual link. The values of hello-multiplier on both ends can be different if at least one Hello packet can be received within dead-interval. You can use the show ip ospf virtual-links command to monitor dead-interval and hello-interval configured for a virtual link.

For the Fast Hello function, you can only configure either the **dead-interval minimal hello-multiplier**

parameter or the **hello-interval** parameter.

Configuration Examples

The following example sets area 1 as the transition area to establish virtual link with neighbor 2.2.2.2.

```
QTECH(config)# router ospf 1
QTECH(config-router)# network 172.16.0.0 0.0.15.255 area0
QTECH(config-router)# network 172.16.17.0 0.0.15.255 area1 QTECH(config-
router)#area1 virtual-link2.2.2.2
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor

1.1.1.1. This virtual link connects area 10 and the backbone area, and works with the OSPF packet authentication in MD5 mode.

```
QTECH(config)# router ospf 1
QTECH(config-router)# network 172.16.17.0 0.0.15.255 area1
```

```
QTECH(config-router)# network 172.16.252.0 0.0.0.255 area10 QTECH(config-router)# area 0
authentication message-digest
QTECH(config-router)# area1 virtual-link 1.1.1.1 message-digest-key 1 md5 hello
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1, enables the Fast Hello function on this virtual link, and sets the multiplier to 3.

```
QTECH(config)# router ospf 1
QTECH(config-router)# network 172.16.17.0 0.0.15.255 area1 QTECH(config-router)#
network 172.16.252.0 0.0.0.255 area10 QTECH(config-router)# area1 virtual-
link 1.1.1.1 dead-interval minimal
hello-multiplier 3
```

Related Commands

Command	Description
area authentication	Enables the OSPF area packet authentication and define the authentication mode.
show ip ospf	Displays the OSPF process information, including the router ID.
show ip ospf virtual-links	Monitors information about a virtual link.

Platform Description

N/A

2.9. auto-cost

Use this command to enable the auto-cost function and set the reference bandwidth according to the reference bandwidth. Use the no form of this command to restore the default setting.

auto-cost [reference-bandwidth *ref-bw*]

no auto-cost [reference-bandwidth]

Parameter Description

Parameter	Description
<i>ref-bw</i>	Reference bandwidth, in the range from 1 to 4294967 Mbps.

Defaults

The default is 100Mbps.

Command Mode

Routing process configuration mode

Usage Guide

By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth.

Run the auto-cost command to obtain the reference value of the auto cost. The default value is 100 Mbps.

Run the bandwidth command to set the interface bandwidth.

The costs of OSPF interfaces on several typical lines are as follows:

64Kbps serial line: The cost is 1562. E1 line: The cost is 48.

10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1.

If you run the ip ospf cost command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Examples

The following example configures the reference bandwidth as 10 Mbps.

```
QTECH(config)# routerospf1
QTECH(config-router)# network172.16.10.0 0.0.0.255 area0
QTECH(config-router)# auto-costreference-bandwidth10
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information
ip ospf cost	Sets the cost value of the OSPF interface.
bandwidth	Sets the interface bandwidth. This setting does not affect data transmission rate.

Platform Description

N/A

2.10. bdf all-interfaces

Use this command to enable Bidirectional Forwarding Detection (BFD) on all OSPF interfaces. Use the **no** form of this command to restore the default setting.

bdf all-interfaces

no bdf all-interfaces

Parameter Description

Parameter	Description
N/A	N/A

Defaults

BDF is disabled by default.

Command Mode

Routing process configuration mode

Usage Guide

OSPF dynamically discovers the neighbors through Hello packets. With the BFD function enabled, one BFD session will be established for the neighbors that match the FULL rules and the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPF will converge with the network immediately.

You can also use the **ip ospf bfd [disable]** command in interface configuration mode to enable or disable the BFD function on the specified interface, which takes precedence over the **bfd all-interfaces** command in routing process configuration mode.

Configuration Examples

```
QTECH(config)# router ospf 1
QTECH(config-router)# bfd all-interfaces
```

Related Commands

Command	Description
router ospf	Creates the OSPF routing process and enters routing process configuration mode.
ip ospf bfd]	Enables the specified interface running OSPF or disabling BFD for link detection.

Platform Description

N/A

2.11. capability opaque

Use this command to enable Opaque LSA. Use the **no** form of this command to disable this function.

capability opaque no capability opaque

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Opaque LSA is enabled by default.

Command Mode

Routing process configuration mode.

Usage Guide

N/A

Configuration Examples

The following example disables Opaque LSA capability.

```
QTECH(config)# router ospf 1
QTECH(config-router)# no capability opaque
```

Related Commands

Command	Description
show ip ospf	Displays the global configuration of OSPF.

Platform Description

N/A

2.12. clear ip ospf process

Use this command to clear and restart the OSPF instance.

clear ip ospf (process-id) process

Parameter Description

Parameter	Description
<i>process-id</i>	<p>OSPF instance ID.</p> <p>When the ID is specified, the command clears data related to the specified instance and restarts the OSPF instance.</p> <p>When no ID is specified, the command clears data related to all running OSPF instances and restarts all the running OSPF instances.</p>

Defaults

The rule recommended in the RFC 1583 is used by default.

Command Mode

Privileged EXEC mode

Usage Guide

Resetting the entire OSPF process causes that all neighbors are re-established and OSPF is greatly affected. Therefore, you are prompted to confirm the execution for deliberation.

Configuration Examples

Related Commands

Platform Description

The following example clears data of OSPF instance 1 and restarts OSPF instance 1.

```
QTECH#clearipospf1process
```

Command	Description
N/A	N/A

N/A

2.13. compatible rfc1583

Use this command to determine the RFC 1583 or RFC 2328 rule for selecting the optimal route among route table several routes to the same destination out of the Autonomous System (AS). **compatible rfc1583**

no compatible rfc1583

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Routing process configuration mode

Usage Guide

N/A

Configuration Examples

The following example determines the best route with the RFC 2328 rule.

```
QTECH(config)# routerospf1
QTECH(config-router)# nocommpatiblerfc1583
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information

Platform Description

N/A

2.14. default-information originate

Use this command to generate a default route to be injected into the OSPF routing domain in routing process configuration mode. Use the **no** form of this command to restore the default setting.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Generates the default route unconditionally, no matter whether the default route exists locally or not.
metric <i>metric</i>	(Optional) Initial metric of the default route in the range from 0 to 16777214
metric-type <i>type</i>	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics on different devices; type 2, same metric on different devices. An external route of type 1 is more trustworthy than that of type 2.
route-map <i>map-name</i>	Associated route map name. No route map is associated by default.

Defaults

No default route is generated by default.

The default value of metric is 1.

The default value of metric-type is 2.

Mode

Usage Guide

When the **redistribute** or **default-information** command is executed, the OSPF-enabled device automatically turns into the ASBR. The ASBR cannot generate the default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR can

generate the default route with the **default-information originate** command in routing process configuration mode.

If the **always** parameter is used, the OSPF routing process advertises an external default route to neighbors, no matter the default route exists or not. However, the local device does not display the default route. To make sure whether the default route is generated, use the **show ip ospf database** command to display the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. You can use the **show ip route** command on the OSPF neighbor to display the default route.

The metric of the external default route can be defined only with the **default-information originate** command.

There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, the type 1 route takes precedence over the type 2 route. As a result, the **show ip route** command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area. To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

The range of set metric is 0 to 16777214 for the associated route map. If the value exceeds the range, introducing a route fails.

Configuration Examples

The following example configures that OSPF generates an external default route and injects it to the OSPF routing domain. The default route is of type 1 and the metric 50.

```
QTECH(config)#routerospf 1
QTECH(config-router)#network172.16.24.0 0.0.0.255 area 0 QTECH(config-
router)#default-information originate
alwaysmetric50metric-type1
```

Related Commands

Command	Description
show ip ospf database	Displays OSPF link state database.
show ip route	Displays the IP route table.
redistribute	Redistributes routes of other routing processes.

Platform Description

2.15. default-metric

Use this command to set the **default metric** of OSPF redistribution route. Use the **no** form of this command to restore the default setting.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
<i>metric</i>	Default metric of the OSPF redistribution route in the range from 1 to 16777214

Defaults

The default metric is not configured by default.

Command Mode

Routing process configuration mode

Usage Guide

The **default-metric** command must work with the **redistribute** command in routing process configuration mode to modify the initial metric of all redistributed routes.

The configuration result of the **default-metric** command does not take effect for the external routes injected into the OSPF routing domain with the **default-information originate** command.

Configuration Examples

The following example configures the default metric of the OSPF redistribution route as 50.

```
Switch(config)# router rip
QTECH(config-router)# network 192.168.12.0
Switch(config-router)# version 2
QTECH(config-router)# exit
QTECH(config)# router ospf 1
QTECH(config-router)# network 172.16.10.0 0.0.0.255 area 0
Switch(config-router)# default-metric 50
QTECH(config-router)# redistribute rip subnets
```

Related Commands

Command	Description
redistribute	Redistributes the routes of other routing processes.
show ip ospf	Displays the OSPF global configuration information.

Platform Description

N/A

2.16. discard-route

Use this command to enable adding the discard-route into the core route table. Use the no form of this command to disable this function.

```
discard-route { internal | external }
```

```
no discard-route { internal | external }
```

Parameter Description

Parameter	Description
internal	Enables adding the discard-route generated with the area range command
external	Enables adding the discard-route generated with the summary-address command.

Defaults

Adding the discard-route is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

After route aggregation, the range may exceed the actual network range of the route table, and sending the data to the nonexistent network may cause loops or increase router loads. To prevent this situation, the discard-route is added to the route table on the ABR or the ASBR. The

discard-route is generated automatically and will not be transmitted.

Configuration Examples

The following example disables adding the discard routes generated with the area range command.

```
QTECH(config)# router ospf 1
QTECH(config-router)# no discard-route internal
```

Related Commands

Command	Description
area range	Configures the route aggregation between OSPF areas.
summary-address	Configures the route aggregation out of the OSPF routing domain.

Platform Description

N/A

2.17. distance ospf

Use this command to set the Administration Distance (AD) of different types of OSPF routes. Use the

no form of this command to restore the default setting.

distance { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**route-map** *map-name*] }

Parameter Description

[**external** *distance*] }

no distance [**ospf**]

Parameter	Description
-----------	-------------

<i>distance</i>	Sets the route AD in the range from 1 to 255.
intra-area <i>distance</i>	Sets the AD of the intra-area route in the range from 1 to 255.
inter-area <i>distance</i>	Sets the AD of the inter-area route in the range from 1 to 255.
External <i>distance</i>	Sets the AD of the external route in the range from 1 to 255.

Defaults

The default value is 110.

The default intra-area distance is 110. The default inter-area distance is 110. The default external distance is 110.

Command Mode

OSPF Routing process configuration mode

Usage Guide

This command is used to specify different ADs for different types of OSPF routes.

Configuration Examples

The following example sets the OSPF external route AD to 160.

```
QTECH(config)# routerospf1
QTECH(config-router)# distance ospf external 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.18. distribute-list in

Use this command to configure LSA filtering. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | *prefix prefix-list-name* [**gateway** *prefix-list-name*] |

route-map *route-map-name* } in [*interface-type interface-number*]

no distribute-list { [*access-list-number* | *name*] | *prefix* *prefix-list-name* [**gateway** *prefix-list-name*] |

route-map *route-map-name* } in [*interface-type* *interface-number*]

Parameter	Description
<i>access-list-number</i> name	Uses the ACL filtering rule.
gateway <i>prefix-list-name</i>	Uses the gateway filtering rule.
Prefix <i>prefix-list-name</i>	Uses the prefix-list filtering rule.
route-map <i>route-map-name</i>	Uses the route-map filtering rule.
<i>interface-type</i> <i>interface-number</i>	Configures the LSA route filtering on the interface.

Defaults

No filtering is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the Shortest Path First (SPF) calculation to generate the corresponding routes. It does not affect the link status database or the route table of the neighbors. It only affects the routing entries calculated by local OSPF. This function is used to control routes that enter the ABR or ASBR.

The following route-map rules will be supported if the route-map parameter is configured:

match interface match ip address

match ip address prefix-list match ip next-hop

match ip next-hop prefix-list match metric

match route-type match tag

Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is

configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the

area filter-list or **area range** (containing the **not-advertise** parameter) command on the ABR to

prevent generation of black-hole routes.

Configuration Examples

The following example configures LSA filtering.

```
QTECH(config)# access-list 3 permit 172.16.0.0 0.127.255
router ospf 25
QTECH(config-router)# distribute-list 3 in ethernet
```

Related Commands

Command	Description
distribute-list out	Filters redistribution routes.

2.19. distribute-list out

Use this command to configure filtering redistribution routes. The function is similar to that of the

redistribute command. Use the no form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | prefix *prefix-list-name* } out [bgp | connected |

isis [*area-tag*] | ospf *process-id* | rip | static]

no **distribute-list** { [*access-list-number* | *name*] | prefix *prefix-list-name* } out [bgp | connected

|isis [*area-tag*] | ospf *process-id* | rip | static]

Parameter Description

Parameter	Description
<i>access-list-number</i> <i>name</i>	Uses the ACL filtering rule.
prefix <i>prefix-list-name</i>	Uses the prefix-list filtering rule.

bgp connected isis [area-tag] ospf process-id rip static	Source of the routes to be filtered
--	-------------------------------------

Defaults

No filtering is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

Similar to the redistribute route-map command, the distribute-list out command filters the routes that other protocols redistribute to the OSPF. However, the distribute-list out command does not redistribute routes by itself. It works with the redistribute command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration, that is, the two rules cannot be configured at the same time for routes from the same source.

Configuration Examples

The following example filters the redistributed static routes.

```
QTECH(config)# routerospf1
QTECH(config)# redistribute static subnets QTECH(config-router)#
distribute-list 22 outstatic
QTECH(config-router)# distribute-list prefix jjj out static
% Access-list filter exists, please de-config first
```

Related Commands

Command	Description
distribute-list in	Configures LSA filtering.
redistribute	Redistributes routes of other routing processes.

2.20. enable mib-binding

Use this command to bind the Management Information Base (MIB) with the specified OSPFv2 process. Use the **no** form of this command to restore the default setting.

enable mib-binding no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The MIB is bound with the OSPFv2 process with the smallest ID by default.

Command Mode

Routing process configuration mode

Usage Guide

OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is bound with the OSPFv2 process with the smallest ID. User operations take effect for this process.

To operate the specified OSPF process over Simple Network Management Protocol(SNMP), use this command to bind the MIB to SNMP.

Configuration Examples

The following example operates OSPFv2 process 100 over SNMP:

```
QTECH(config)# routerospf100
QTECH(config-router)# enable mib-binding
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable traps	Configures the OSPF TRAP function.

Platform Description

N/A

2.21. enable traps

The OSPFv2 process supports 16 kinds of TRAP packets, which are classified into four categories. Use this command to enable sending the specified TRAP messages. Use the **no** form of this command to restore the default setting.

```
enable traps [ error [ IfAuthFailure | IfConfigError | IfRxBadPacket | VrtIfAuthFailure |
VrtIfConfigError | VrtIfRxBadPacket ] | lsa [ LsdbApproachOverflow | LsdbOverflow |
MaxAgeLsa | OriginateLsa ] | retransmit [ IfTxRetransmit | VrtIfTxRetransmit ] | state-
change
```

Parameter Description

```
[ IfStateChange | NbrRestartHelperStatusChange | NbrStateChange |
NssaTranslatorStatusChange | RestartStatusChange | VrtIfStateChange |
VrtNbrRestartHelperStatusChange | VrtNbrStateChange ] ]
```

```
no enable traps [ error [ IfAuthFailure | IfConfigError | IfRxBadPacket | VrtIfAuthFailure |
VrtIfConfigError | VrtIfRxBadPacket ] | lsa [ LsdbApproachOverflow | LsdbOverflow |
MaxAgeLsa | OriginateLsa ] | retransmit [ IfTxRetransmit | VrtIfTxRetransmit ] | state-
change [ IfStateChange | NbrRestartHelperStatusChange | NbrStateChange |
NssaTranslatorStatusChange | RestartStatusChange | VrtIfStateChange |
VrtNbrRestartHelperStatusChange | VrtNbrStateChange ] ]
```

Parameter	Description
error	Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches.
	lfauthfailure Interface authentication error
	ifconfigerror Interface parameter configuration error
	lfrxbadpacket Error packets received on the interface
	Vrtifauthfailure Authentication error on the virtual interface
	Vrtifconfigerror Parameter configuration error on the virtual interface
	Vrtifrxbadpacket Error packets received on the virtual interface
	Configures all traps switches related to the LSA. Use this parameter

isa	to set the following specified LSA traps switches.	
	Lsdbapproachoverflow	External LSA count has reached the 90% of the upper limit.
	Lsdboverflow	External LSA count has reached the upper limit.
	Maxagelsa	LSA reaching the aging time
	Originatelsa	Generates new LSA
retransmit	Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches.	
	lftxretransmit	Packet retransmission on the interface
	Virtiftxretransmit	Packet retransmission on the virtual interface
state-change	Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches.	
	Ifstatechange	Interface state change
	NbrRestartHelperStatusChange	State change during the neighbor GR process
	Nbrstatechange	Neighbor state change
	NssaTranslatorStatusChange	State change of the NSSA translator
	RestartStatusChange	State change of the GR Restarter on the device
	Virtifstatechange	State change on the virtual interface

	VirtNbrRestartHelper StatusChange	Status change of the virtual neighbor GR process
	Virtnbrstatechange	State change on the virtual neighbor

Defaults

All TRAP switches are disabled by default.

Command Mode

Routing process configuration mode

Usage Guide

The `snmp-server enable traps ospf` command must be configured before you configure this command, for it is limited by the `snmp-server` command.

This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Configuration Examples

The following example enables all TRAP switches of OSPFv2 process 100.

```
QTECH(config)# routerospf100
QTECH(config-router)# enable traps
```

Related Commands

Command	Description
<code>show ip ospf</code>	Displays the OSPF global configuration information.
<code>enable mib-binding</code>	Binds the OSPFv2 process with MIB.
<code>snmp-server enable traps ospf</code>	Enables the OSPF TRAP notification function.

Platform Description

N/A

2.22. fast-reroute

Use this command to enable the OSPF FRR (Fast Reroute) function for the device. Use the no form of this command to restore the default setting.

```
fast-reroute { lfa | downstream-paths | route-map route-map-name }
```

```
no fast-reroute { lfa [ downstream-paths ] | route-map }
```

Parameter Description

Parameter	Description
lfa	Enables the LFA (loop-free alternate) path computation.
downstream-paths	Enables the downstream path computation.
route-map <i>route-map-name</i>	Specifies the backup path through the route map.

Defaults

The FRR function is disabled by default.

Command Mode

Routing process configuration mode

Usage Guide

If the **lfa** parameter is configured, computation of the loop-free standby path is enabled. In this case, you can use the interface mode command to specify the path protection mode of the interface.

It is recommended that computation of the loop-free standby path be disabled if any of the following case exists on the network:

Virtual links exist.

Alternative ABRs exist.

An ASBR is also an ABR.

Multiple ASBRs advertise the same external route.

If both **lfa** and **downstream-paths** are configured, computation of the downstream path is enabled.

If **route-map** is configured, a standby path can be specified for a matched route through the route-map.

When the OSPF fast reroute function is used, it is recommended that BFD be enabled at the same time so that the device can quickly detect any link failure and therefore shorten the forwarding interruption time. If the interface is up or down, to shorten the forwarding interruption time during OSPF fast reroute, you can configure **carrier-delay 0** in L3 interface configuration mode to achieve the fastest switchover speed.

Configuration Examples

The following example enables FRR for OSPF instance 1 and associates route map *fast reroute*.

```

QTECH(config)# route-map fast-reroute
QTECH(config-route-map)# match ip address 1
QTECH(config-route-map)# set fast-reroute backup-nexthop GigabitEthernet 0/1 backup-nexthop
192.168.1.2
QTECH(config)# router ospf 1
QTECH(config-router)# fast-reroute route-map fast-reroute

```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPF graceful-restart helper.

Platform Description

N/A

2.23. graceful-restart

Use this command to enable the graceful restart (GR) of OSPF on the device. Use the **graceful-restart grace-period** command to configure the grace period parameter and enable the OSPF GR function. Use the **no** form of this command to disable this function.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [*graceful-period*]

Parameter Description

Parameter	Description
grace-period <i>grace-period</i>	Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is 120s.
inconsistent-lsa-checking	Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete

	convergence. After GR is enabled, topological change detection is enabled by default.
--	---

Defaults

This function is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

GR is configured based on the OSPF instance. Different instances could be configured with different parameters according to the actual situation.

The graceful restart interval is the longest time between the OSPF restart and the graceful restart. In this period, you can perform link status reconstruction to restore the OSPF status to the original. With the interval times out, the OSPF will exit GR and perform common OSPF operations.

The GR interval is 120 seconds set with the graceful-restart command, and the graceful-restart grace-period command allows you to change the interval explicitly.

GR is unavailable when the Fast Hello function is enabled.

Configuration Examples

The following example enables GR for the OSPF instance 1 and sets the restart interval for GR.

```
QTECH(config)# router ospf 1 QTECH(config-router)#  
graceful-restart  
QTECH(config-router)# graceful-restart grace-period 60
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPF graceful-restart helper.

Platform Description

N/A

2.24. graceful-restart helper

Use this command to enable the graceful restart helper function. Use the no form of this command to restore the default setting.

graceful-restart helper disable

no graceful-restart helper disable

Parameter Description

graceful-restart helper { strict-lsa-checking | internal-lsa-checking } no graceful-restart helper {strict-lsa-checking | internal-lsa-checking}

Parameter	Description
disable	Prohibits a device from acting as a GR helper for another device.
strict-lsa-checking	Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
internal-lsa-checking	Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.

Defaults

The GR helper is enabled by default.

The router enabled with the GR helper does not check the LSA change by default.

Command Mode

Routing process configuration mode

Usage Guide

This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving

the Grace-LSA, and helps the neighbor to complete GR. The `disable` option indicates that GR helper is not provided for any device that implements GR.

After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure `strict-lsa-checking` to check Type 1 to 5 and Type 7 LSAs that indicate the network information or `internal-lsa-checking` to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (`strict-lsa-checking` and `internal-lsa-checking`) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration Examples

The following example disables the GR helper and modifies the policy of checking network changes.

```
QTECH(config)# router ospf1
QTECH(config-router)# graceful-restart helper disable
QTECH(config-router)# no graceful-restart helper disable
QTECH(config-router)# graceful-restart helper
strict-lsa-checking
```

Related Commands

Command	Description
<code>graceful-restart</code>	Enables GR on the device.

Platform Description

N/A

2.25. ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of this command to restore the default setting.

`ip ospf authentication [message-digest | null]`

no ip ospf authentication

Parameter Description

Parameter	Description
message-digest	Enables MD5 authentication on the interface.

null	Enables no authentication.
-------------	----------------------------

Defaults

No authentication mode is configured and that of the local area is used on the interface by default.

Command Mode

Interface configuration mode

Usage Guide

Plaintext authentication is applicable when **no** option is used with the command. Note that the no form of this command restores the default value. Whether authentication is used actually depends on authentication mode configured for the local area of the interface. If authentication mode is configured as **null**, no authentication is enabled. When both the interface and its area are configured with authentication, the one for the interface takes precedence.

Configuration Examples

The following example configures MD5 authentication for OSPF on fastEthernet 0/1.

```
QTECH (config)#interface fastEthernet0/1
QTECH(config-if-FastEthernet 0/1)# ipaddress172.16.1.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf authentication
message-digest
```

Related Commands

Command	Description
area authentication	Enables authentication and defines authentication mode in the OSPF area.
ip ospf authentication-key	Configures the plain text authentication key.
ip ospf message-digest-key	Configures the MD5 authentication key.

Platform Description

N/A

2.26. ip ospf authentication-key

Use this command to configure the OSPF plain text authentication key in interface configuration mode. Use the no form of this command to restore the default setting.

```
ip ospf authentication-key [ 0 | 7 ] key
```

```
no ip ospf authentication-key
```

Parameter Description

Parameter	Description
0	Displays the key in plain text.
7	Displays the key in cipher text.
key	Key containing at most eight characters.

Defaults

It is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

The **ip ospf authentication-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys may vary by interface, but the devices that are connected to the same physical network segment must use the same key.

To enable the OSPF area authentication, execute the area authentication command in routing process configuration mode.

The authentication can be enabled separately on an interface by executing the ip ospf authentication command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

Configuration Examples

The following example configures the OSPF authentication key ospfauth for fast Ethernet 0/1.

```
QTECH (config)#interfacefastEthernet0/1
QTECH(config-if-FastEthernet 0/1)# ipaddress172.16.1.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode
ip ospf authentication	Enables authentication on the interface and defines authentication mode

Platform Description

N/A

2.27. ip ospf bfd

Use this command to enable or disable the BFD on the specified OSPF interface. Use the **no** form of this command to restore the default setting.

```
ip rip bfd [ disable ]
```

```
no ip ospf bfd
```

Parameter Description

Parameter	Description
disable	Disables BFD on the specified OSPF interface.

Defaults

BFD is not configured by default, and the BFD configuration in OSPF process configuration mode shall prevail.

Command Mode

Interface configuration mode

Usage Guide

The interface-based configuration takes precedence over the **bfd all-interfaces** command used in process configuration mode.

Based on the actual environment, you can run the **ip ospf bfd** command to enable BFD on a specified interface for link detection, or run the **bfd all-interfaces** command in OSPF process configuration mode to enable BFD on all interface of the OSPF process, or run the **ospf bfd disable** command to disable BFD on a specified interface.

Configuration Examples

```
QTECH(config)# interface fastethernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf bfd
```

Related Commands

Command	Description
router ospf	Creates the OSPF routing process and enters routing process configuration mode.
bfd all-interfaces	Enables the BFD on all OSPF interfaces.

Platform Description

N/A

2.28. ip ospf cost

Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in interface configuration mode. Use the **no** form of this command to restore the default setting.

Parameter Description

ip ospf cost *cost*

no ip ospf cost

Parameter	Description
<i>cost</i>	OSPF interface cost in the range from 0 to 65535

Defaults

The default interface cost is calculated as follows: Reference bandwidth/Bandwidth

The reference bandwidth is 100 Mbps by default.

Command Mode

Interface configuration mode

Usage Guide

By default, the OSPF interface cost is 100Mbps/Bandwidth, where Bandwidth is the interface bandwidth configured with the bandwidth command in interface configuration mode.

The default costs of different types of lines are as follows:

64K serial line: 1562

E1 line: 48

10M Ethernet: 10

100M Ethernet: 1

The OSPF cost configured with the ip ospf cost command will overwrite the default configuration.

Configuration Examples

The following example configures the OSPF cost of fastEthernet 0/1 to 100.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip ospf cost 100
```

Related Commands

Command	Description
bandwidth	Specifies the interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Displays the OSPF global configuration information

Platform Description

N/A

2.29. ip ospf database-filter all out

Use this command to stop advertising LSAs of an interface, that is, the LSA update packets are not sent on the interface. Use the **no** form of the command to restore the default setting.

ip ospf database-filter all out

no ip ospf database-filter

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled and all LSA update packets can be sent on the interface by default.

Command Mode

Interface configuration mode

Usage Guide

To stop sending LSA update packets on the interface, enable this function on the interface. Then, the device maintains the neighboring connections and accepts LSAs from neighbors, but stops sending LSAs to neighbors.

Configuration Examples

The following example stops sending LSA update packets of fastEthernet 0/1.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf database-filter all out
```

Related Commnds

Command	Description
N/A	N/A

Platform Description

N/A

2.30. ip ospf dead-interval

Use this command to configure the interval for determining the death of an interface neighbor in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf dead-interval { *seconds* | **minimal hello-multiplier** *multiplier* }

no ip ospf dead-interval

Parameter Description

Parameter	Description
<i>seconds</i>	Defines the interval for determining the neighbor death in seconds. The range is from 0 to 2,147,483,647.
minimal	Indicates that the Fast Hello function is enabled to set the dead interval to 1s.
hello-multiplier <i>multiplier</i>	Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20.

Defaults

The value of dead-interval is 4 times the interval configured with the **ip ospf hello-interval** command by default.

Command Mode

Interface configuration mode

Usage Guide

The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically.

When using this command to manually modify the dead interval, pay attention to the following issues:

The dead interval cannot be shorter than the Hello interval.

The dead interval must be the same on all routers in the same network segment.

2.31. OSPF supports the Fast Hello function.

After the OSPF Fast Hello function is enabled, OSPF finds neighbors and detects neighbor failures faster. You can enable the OSPF Fast Hello function by specifying the **minimal** and **hello-multiplier** keywords and the **multiplier** parameter. The **minimal** keyword indicates that the death interval is set to 1s, and **hello-multiplier** indicates the number of Hello packets sent per second. In this way, the interval at which the Hello packet is sent decreases to less than 1s.

If the Fast Hello function is configured for a virtual link, the Hello interval field of the Hello packet advertised on the virtual link is set to 0, and the Hello interval field of the Hello packet received on this virtual link is ignored.

No matter whether the Fast Hello function is enabled, the death interval must be consistent and the **hello-multiplier** values can be inconsistent on routers at both ends of the virtual link. Ensure that at least one Hello packet can be received within the death interval.

Run the **show ip ospf virtual-links** command to monitor the death interval and Fast Hello interval configured for the virtual link.

The **dead-interval minimal hello-multiplier** and **hello-interval** parameters introduced for the Fast Hello function cannot be configured simultaneously.

Configuration Examples

The following example configures the interval for determining the death of the OSPF neighbor on fastEthernet 0/1 to 30 seconds.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf dead-interval 30
```

The following example configures the value of hello-multiplier to 3.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf dead-interval minimal hello-multiplier 3
```

Related Commands

Command	Description
ip ospf hello-interval	Specifies the interval at which the OSPF sends Hello packets
show ip ospf interface	Displays OSPF interface information.

Platform Description

N/A

2.32. ip ospf disable all

Use this command to prevent the specified interface from generating OSPF packets. Use the **no** form of this command to restore the default setting.

ip ospf disable all

no ip ospf disable all**Parameter Description**

Parameter	Description
N/A	N/A

Defaults

OSPF packets are generated on the specified interface by default.

Command Mode

Interface configuration mode

Usage Guide

The interface configured with this command will ignore whether the network areas are matched. After this command is configured, an interface will not generate OSPF packets even if the interface belongs to the network; therefore, the interface does not receive or send any OSPF packets or participate in OSPF calculation.

Configuration Examples

The following example prevents the specified interface from generating OSPF packets.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf disable all
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.33. ip ospf fast-reroute protection

Use this command to specify the loop-free alternate (LFA) protection mode for an interface. Use the

Parameter Description

Parameter	Description
node	Enables LFA node protection.
link-node	Enables LFA link node protection.
disable	Disables LFA protection.

no form of this command to restore the default setting.

`ip ospf fast-reroute protection { node | link-node | disable }`

no ip ospf fast-reroute protection

Defaults

LFA node protection is enabled by default.

Command Mode

Interface configuration mode

Usage Guide

Enabling the **fast-reroute lfa** command in OSPF process configuration mode will enable OSPF fast reroute and generate a backup route for the master route according to the specified LFA protection mode in interface configuration mode. By default, link protection is enabled on each OSPF interface. In this protection mode, the failure of a master link does not affect forwarding on the backup route. Use the **node** parameter to enable node protection for an interface, that is, the neighbor node of a master link does not affect forwarding on the backup route.

Similarly, use the **link-node** parameter to protect the link and neighbor link of a master route at the same time.

Use the **disable** parameter to disable the LFA protection function for an interface, that is, a backup entry is not generated for the routes with this interface as the next hop.

Configuration Examples

The following example sets OSPF LFA fast reroute to link and node protection:

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf fast-reroute protection link-node
```

Related Commands

Command	Description
---------	-------------

fast-reroute	Enables OSPF fast reroute.
---------------------	----------------------------

Platform Description

N/A

2.34. ip ospf fast-reroute no-eligible-backup

Use this command in interface configuration mode to exclude an OSPF interface as a backup interface in OSPF fast reroute calculation. Use the **no** form of this command to restore the default

Parameter Description

Parameter	Description
N/A	N/A

setting.

`ip ospf fast-reroute no-eligible-backup`

`no ip ospf fast-reroute no-eligible-backup`

Defaults

An OSPF interface can serve as a backup interface by default.

Command Mode

Interface configuration mode

Usage Guide

If the remaining bandwidth of an interface is small or if the interface and its active interface may fail at the same time, the interface cannot be used as a standby interface. Therefore, you need to run this command in interface configuration mode to prevent this interface from becoming a standby interface during OSPF fast reroute computation. After this command is executed, the standby interface is selected from other interface.

This command does not take effect if **fast-reroute route-map** is configured.

Configuration Examples

The following example excludes FastEthernet 0/1 as a backup interface in OSPF fast reroute calculation.

```
QTECH(config)# interface fastEthernet 0/1
```

```
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf fast-reroute no-eligible-backup
```

Related Commands

Command	Description
fast-reroute	Enables OSPF fast reroute.

Platform Description

N/A

2.35. ip ospf hello-interval

Use this command to set the interval for sending Hello packets in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter Description

Parameter	Description
<i>seconds</i>	Interval for sending Hello packets in seconds. The range is from 1 to 65535.

Defaults

The defaults are as follows:

10seconds for Ethernet

10seconds for PPP or HDLC encapsulated interfaces 10seconds for frame relay PTP interfaces

30seconds for non-frame relay PTP sub-interface and X.25 interfaces

Command Mode

Interface configuration mode

Usage Guide

The interval of sending the Hello packets is included in the Hello packet. A shorter interval means that OSPF detects the topological change faster, which will increase network traffic.

The Hello packet sending intervals for all the devices in the same network segment must be the same. To manually modify the interval to determine neighbor death, ensure that the Hello packet sending interval cannot be greater than dead-interval of the neighbor.

Configuration Examples

The following example configures the interval of sending the Hello packets on fastEthernet 0/1 to 15.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf hello-interval 15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the interval for determining the death of the OSPF neighbor.

Platform Description

N/A

2.36. ip ospf message-digest-key

Use this command to configure the MD5 authentication key in interface configuration mode. Use the

no form of this command to restore the default setting. **ip ospf message-digest-key** *key-id* **md5** [**0** | **7**] *key* **no ip ospf message-digest-key** *key-id*

Parameter Description

Parameter	Description
<i>key</i>	Key of up to 16 characters
0	Displays the key in plain text.
7	Displays the key in cipher text.
<i>key-id</i>	Key identifier in the range from 1 to 255

Defaults

No MD5 key is configured by default.

Command Mode

Interface configuration mode

Usage Guide

The **ip ospf message-digest-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighboring relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key. For neighbors, the same key identifier must correspond to the same key.

To enable OSPF area authentication, execute the **area authentication** command in routing process configuration mode. The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

The software supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF packets by using different keys, till it confirms that the neighbors have been configured with new keys. When all devices have been configured with new keys, it is possible to delete the old key.

Configuration Examples

The following example adds a new OSPF authentication key "hello5" with key ID 5 for fastEthernet 0/1.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0
QTECH(config-if-FastEthernet 0/1)# ip ospf authentication message-digest
QTECH(config-if-FastEthernet 0/1)# ip ospf message-digest-key 10 md5 hello10
QTECH(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5md5 hello5

QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# no ip ospf message-digest-key10md5
hello10
```

When all neighbors are added with new keys, the old keys shall be deleted for all devices.

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines

	authentication mode.
ip ospf authentication	Enables authentication on the interface and defines authentication mode.

Platform Description

N/A

2.37. ip ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database description packet. Use the no form of this command to restore the default setting.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults

MTU check is disabled by default.

Command

Mode

Interface configuration mode

Usage Guide

After receiving the database description packet, the device will check whether the MTU of the neighbor interface is the same as its own MTU. If the received database description packet indicates an MTU greater than the interface's MTU, the neighboring relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration Examples

The following example disables the MTU check function on fastEthernet 0/1.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip ospf mtu-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.38. ip ospf network

Use this command to configure the OSPF network type in interface configuration mode. Use the **no**

form of this command to restore the default setting.

ip ospf network { broadcast | non-broadcast |

point-to-multipoint [non-broadcast] | point-to-point }

no ip ospf network

Parameter Description

Parameter	Description
broadcast	Sets the OSPF network type as the broadcast type.
non-broadcast	Sets the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
point-to-multipoint [non-broadcast]	Sets the OSPF network type as the point-to-multipoint type. The value is the point-to-multipoint broadcast type by default. The non-broadcast option means the point-to-multipoint non-broadcast type.
point-to-point	Sets the OSPF network type as the point-to-point type.

Defaults

The default configurations are as follows:

PTP network type: Point-to-Point Protocol(PPP), Serial Line Internet Protocol(SLIP), frame relay point-to-point (PTP) sub-interface, X.25 PTP sub-interface encapsulation

NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface)

Broadcast network type: Ethernet encapsulation

By default, the network type is the point-to-multipoint network type.

Command Mode

Interface configuration mode

Usage Guide

The broadcast type requires that the interface must have the broadcast capability.

The P2P type requires that the interfaces are interconnected in one-to-one manner.

The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.

The P2MP type does not raise any requirement.

Configuration Examples

The following example configures the frame relay interface network as the P2P type.

```
QTECH(config)# interface Serial 1/0
QTECH(config-Serial 1/0)#ip address 172.16.24.4 255.255.255.0 QTECH(config-Serial
1/0)# encapsulation frame-relay QTECH(config-Serial 1/0)# ip ospf network point-
to-point

QTECH(config)# interface Serial 1/0
QTECH(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0 QTECH(config-Serial
1/0)# encapsulation frame-relay QTECH(config-Serial 1/0)# ip ospf network non-
broadcast QTECH(config-Serial 1/0)#exit
QTECH(config)# router ospf 20
QTECH(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

The following example configures the frame relay interface network as the NBMA type.

Related Commands

Command	Description
---------	-------------

dialer map ip	Defines the mapping between IP address and dialing number.
frame-relay map	Defines the mapping between IP address and
	frame DLCI.
neighbor (OSPF)	Defines the IP address of neighbor applicable to NBMA network type and point-to-multipoint non-broadcast type only.
X25 map	Defines the mapping between IP address and X.25 network address.

Platform Description

N/A

2.39. ip ospf priority

Use this command to configure the OSPF priority in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf priority *priority*

no ip ospf priority

Parameter Description

Parameter	Description
<i>priority</i>	Sets the OSPF priority of the interface in the range from 0 to 255.

Defaults

The default is 1.

Command Mode

Interface configuration mode

Usage Guide

The interface priority is included in the Hello packet. When DR/BDR election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid only for OSPF broadcast and non-broadcast network types.

Configuration Examples

The following example configures the priority of fastethernet 0/1 as 0.

```
Switch(config)#interface fastethernet 0/1
QTECH(config-if-FastEthernet 0/1)# ipospfpriority0
```

Related Commands

Command	Description
ip ospf network	Configures the network type of the interface.

Platform Description

N/A

2.40. ip ospf retransmit-interval

Use this command to define the interval for sending the link state update (LSU) packet on the interface in interface configuration mode. Use the no form of this command to restore the default setting.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter Description

Parameter	Description
<i>seconds</i>	Interval for sending the LSU packets in seconds. The range is from 1 to 65535. This interval must be greater than the round trip delay of packets between two neighbors.

Defaults

The default is 5.

Command Mode

Interface configuration mode

Usage Guide After the device sends an LSU packet, the LSU packet stays in the transmission buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the `ip ospf retransmit-interval` command, the LSU will be sent once again.

In serial lines or virtual links, the retransmission interval shall be slightly larger. The LSU packet retransmission interval of virtual links is defined with the `area virtual-link` command followed with the keyword `retransmit-interval`.

Configuration Examples

The following example configures the LSU packet retransmission interval on fastEthernet 0/1 as 10 seconds.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform Description

N/A

2.41. ip ospf source-check-ignore

Use this command to disable the source address check in the point-to-point link. Use the **no** form of this command to restore the default setting

`ip ospf source-check-ignore`

`no ip ospf source-check-ignore`

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode

Usage Guide

For OSPF, the source address of the received packet is required to be in the same network segment with the receiving interface. However, in a point-to-point link, the addresses of two ends of the link are individually set, and they are not required to be in the same network segment. The peer address is informed during the process of point-to-point link negotiation; therefore, OSPF will check whether the source address of the packet is the informed one. If no, the OSPF regards this packet as illegal and drops it. In some applications, the addresses informed during the negotiation are shielded. You need to disable the source address check to ensure the normal establishment of OSPF neighbors. The source address check shall be never enabled, especially for the unnumbered interfaces.

Configuration Examples

The following example disables the source address check function in the point-to-point link.

```
QTECH(config)# interface serial 1/0
QTECH(config-if)# ip ospf source-check-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.42. ip ospf subvlan

Use this command to enable OSPF on super VLANs. Use the **no** form of this command to restore the default setting.

```
ip ospf subvlan [all | vid] no ip ospf subvlan
```

Parameter Description

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
<i>vid</i>	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults

The default setting takes effect only on super VLANs with OSPFv3 disabled.

Command Mode

Interface configuration mode

Usage Guide

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the OSPF function does not need to be enabled on a super VLAN. Therefore, the OSPF function is disabled by default. However, in some scenarios, the OSPF function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flap.

Configuration Examples

The following example sends OSPF multicast packets to sub VLAN 1024 of super VLAN 300.

```
QTECH(config)# interface vlan 300
QTECH(config-if-VLAN 300)# ip ospf subvlan 1024
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.43. ip ospf transmit-delay

Use this command to define the LSU packet transmission delay in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter Description

Parameter	Description
<i>seconds</i>	LSU packet transmission delay in seconds in the range from 1 to 65535.

Defaults

The default is 1.

Command Mode

Interface configuration mode

Usage Guide

Before the LSU packet is transmitted, the Age field in all the LSAs of the packet will be increased by the value defined with the **ip ospf transmit-delay** command in interface configuration mode. The configuration of this parameter shall consider the transmission and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU packet transmission delay of the virtual link is defined with the **area virtual-link** command followed with the keyword **retransmit-interval**.

The software will resend or request resending the LSA with Age up to 3600. If no update is obtained in time, the aged LSA will be cleared from the link state database.

Configuration Examples

The following example configures the transmission delay of fastEthernet 0/1 as 10.

```
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform Description

N/A

2.44. ispf enable

Use this command to enable the ISPF function. Use the no form of this command to disable the ISPF function.

ispf enable no ispf enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

ISPF is disabled by default.

Command

Mode Routing process configuration mode

Usage Guide

OSPF adopts the SPF algorithm to calculate the network topology within an area. SPF algorithm is run for each area independently,

Incremental SPF algorithm (ISPF) is an area-based algorithm. If the topology changes, the ISPF algorithm will calculate only the affected nodes of the topology rather than calculating the entire tree, which speeds up the OSPF route convergence and saves CPU resources.

Because the ISPF algorithm is not shared among routers, each router within the same network can have a unique ISPF algorithm. To ensure a faster OSPF convergence, the ISPF function should be

enabled on every router within the network.

Enabling ISPF function only affects the choice of topology calculating algorithm for OSPF. So you can configure the delay time for the ISPF with the timers spf command and the timers throttle spf command as well.

Configuration Examples

The following example enables the ISPF function.

```
QTECH(config)# router ospf 1
QTECH(config-router)# ispf enable
```

```
QTECH(config)# router ospf 1 vrf vpn1
QTECH(config-router)# ispf enable
```

The following example enables the ISPF function on the specified VRF.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.45. log-adj-changes

Use this command to enable the logging of the neighbor state changes. Use the **no** form of the command to disable this function.

log-adj-changes [detail]

no log-adj-changes [detail]

Parameter Description

Parameter	Description
detail	Records the detail of changes.

Defaults

This function is enabled by default. Without the detail parameter, the system records the logs that the neighbor enters or exits the full state.

Command Mode

Routing process configuration mode

Usage Guide

N/A

Configuration Examples

The following example logs the neighbor state changes.

```
QTECH(config)# router ospf 1
QTECH(config-router)# log-adj-changes detail
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.

Platform Description

N/A

2.46. max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description

Parameter	Description
<i>number</i>	Maximum number of DD packets in the range from 1 to 65535

Defaults

The default is 5.

Command Mode

Routing process configuration mode

Usage Guide

When a router is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have at the same time.

Configuration Examples

The following example sets the maximum number of DD packets to 4.

After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
QTECH(config)# routerospf10
QTECH(config-router)# max-concurrent-dd4
```

Related Commands

Command	Description
router ospf max-concurrent-dd	Sets the maximum number of neighbors allowed in concurrent interaction for all OSPF routing processes.

Platform Description

N/A

2.47. max-metric

Use this command to set the maximum metric of the router-lsa, so that this routing device will not firstly be used as the transmission node by other devices in SPF computing. Use the **no** form of this command to restore the default setting.

max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** [*seconds*]]

[**summary-lsa** [*max-metric-value*]]

no max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** [*seconds*]] [**summary-lsa** [*max-metric-value*]]

Parameter Description

Parameter	Description
-----------	-------------

router-lsa	Configures the maximum metric (0XFFFF) of non-stub links in the Router LSA.
external-lsa	Uses the maximum metric instead of the external-lsa metric (including the Type-5 and Type-7).
<i>max-metric-value</i>	Maximum metric of the LSA. The range is 1 to 16777215. The default value is 16711680,
include-stub	Configures the maximum metric of the stub links in the Router LSA.
on-startup	Advertises the maximum metric when the routing device starts up.
<i>seconds</i>	Interval of advertising the maximum metric. The range is 5 to 86400. The default value is 600 seconds.
summary-lsa	Uses the maximum metric to replace the summary LSA metric. (including Type-3 and Type-4)

Defaults

The normal metric LSAs are used by default.

Command Mode

Routing process configuration mode

Usage Guide

With the **max-metric router-lsa** command enabled, the maximum metric of non-stub links in the Router LSA generated by the routing device is set. The link's normal metric is restored after canceling this configuration or reaching the timer.

By default, with this command enabled, the normal metric of the stub links is still advertised, which is the output interface cost. If the **include-stub** parameter is configured, the maximum metric of the stub links will be advertised.

When the device acts as an ABR, if no interval flow transmission is expected, use the **summary-lsa**

parameter to set the summary LSA as the maximum metric.

When the device acts as an ASBR device, if no external flow transmission is expected, use the

external lsa parameter to set the external LSA as the maximum metric.

The **max-metric router-lsa** command is usually used in the following scenes:

The device is restarted, which generally makes the IGP protocol converge faster, so that other devices attempt forwarding the dataflow through the new started-up device. If the current device remains establishing a BGP routing table, the packets sent to these networks will be discarded due to some BGP routings have not been learned. In this case, use the **on-startup** parameter to set certain delay, so that this device can serve as a transmission node after restarting.

The device is added into the network without being used for dataflow transmission. If the backup path exists, the current device is not used for the dataflow transmission. Otherwise, this device is still used to transmit the dataflow.

Remove the device from the network gracefully. With this command enabled, the current device advertises the maximum metric to all devices, as that the other devices in this network can choose the backup path to for the dataflow transmission before the current device is removed.

For the OSPF implementation in the earlier versions (RFC 1247 or earlier versions), the links with the maximum metric (0xFFFF) in the LSA will not participate in the SPF calculation, that is,

no dataflow will be sent to the router that have generated these LSAs.

Configuration Examples

The following example configures the LSA maximum metric as 100 seconds after starting the device.

```
QTECH(config)# router ospf 20
QTECH(config-router)# max-metric router-lsa on-startup 100
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF related configurations.

Platform Description

N/A

2.48. neighbor

Use this command to define the OSPF neighbor in routing process configuration mode. Use the **no**

form of this command to restore the default setting.

Neighbor *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost*]

no neighbor *ip-address* [[**poll-interval**] [**priority**] [**cost**]]

Parameter Description

Parameter	Description
ip address	IP address of the neighbor
poll-interval seconds	(Optional) Specifies the interval of polling neighbors in seconds. The range is from 0 to 2147483647. Only the non-broadcast (NBMA) network type supports this option.
priority priority	(Optional) Configures the priority of non-broadcast network neighbors. The range is from 0 to 255. Only the non-broadcast (NBMA) network type supports this option.
cost cost	(Optional) Configures the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. The range is from 0 to 65535. Only the point-to-multipoint [non-broadcast] network type supports
	this option.

Defaults

No neighbor is defined by default.

The default neighbor polling interval is 120 seconds. The default NBMA neighbor priority is 0.

Command Mode

Routing process configuration mode

Usage Guide

The software must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface.

In the NBMA network, if the neighbor device becomes inactive, in other words, if the Hello packet is not received within the device dead-interval, the OSPF will send more Hello

packets to the neighbor. The interval at which the Hello packets are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello packets only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello packets to all neighbors to establish the neighbor relationship.

Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the cost option for the point-to-multipoint network type.

Configuration Examples

The following example declares an OSPF non-broadcast network neighbor, with the IP address 172.16.24.2, priority 1 and polling interval 150 seconds.

```
QTECH(config)# routerospf 20
QTECH(config-router)# network 172.16.24.0 0.0.0.255 area 0
QTECH(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
ip ospf priority	Sets the interface priority.
ip ospf network	Sets the network type

Platform Description

N/A

2.49. nsr

Use this command to enable the nonstop routing (NSR) function for the OSPF instance. Use the **no**

form of this command to disable the NSR function.

nsr

no nsr

Parameter Description

Parameter	Description
N/A	N/A

Defaults

NSR is disabled by default.

Command Mode

Routing process configuration mode

Usage Guide

NSR enables the device to recover link state and regenerate routes without the assistance from neighbors during active/standby switchover of distributed devices or VSU system. The backup information includes adjacencies and OSPF state.

You need to enable either NSR or GR in the same OSPF process. That is, the NSR feature will be disabled after the GR feature is enabled. Similarly, the GR feature will be disabled after NSR is enabled, and the GR Helper capability is still supported.

The active/standby switchover of distributed devices or VSU system takes a period of time. If the OSPF dead interval is less than the switchover period, OSPF neighbors will be disconnected and the services will be interrupted. It is recommended to configure the OSPF dead interval longer than its default value. It is not recommended to enable the Fast Hello feature after NSR is enabled, because OSPF dead interval is less than 1 second when the Fast Hello feature is enabled and the OSPF neighbors are disconnected and NSR becomes ineffective.

Configuration Examples

The following example enables NSR.

```
QTECH(config)#router ospf 1
QTECH(config-router)# nsr
```

Related Commands

Command	Description
router ospf	Creates the OSPF routing process.

Platform Description

N/A

2.50. network area

Use this command to define which interfaces run OSPF and the OSPF areas they belong to in routing process configuration mode. Use the **no** form of this command to restore the default setting. **network** *ip-address wildcard area area-id*

no network *ip-address wildcard area area-id*

Parameter Description

wildcard	Defines the comparison bits in the IP address, with 0 for exact match and 1 for no comparison
area-id	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as the OSPF area identifier.
Parameter	Description
ip-address	IP address of the interface

Defaults

No OSPF area is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

The ip-address and wildcard parameters allow associating multiple interfaces with one OSPF area.

To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by the network area command.

You can determine the OSPF process that the interface takes part in by the means of the best match if the IP address of the interface matches the IP address ranges defined by the network command in multiple OSPF processes.

Configuration Examples

The following example defines:

Three areas: 0, 1 and 172.16.16.0

The interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1 The interfaces whose IP addresses fall into the

2. OSPFv2 Commands

172.16.16.0/20 range to area 2 The remaining interface being assigned to area 0.

```
QTECH(config)# routerospf 20
QTECH(config-router)# network172.16.16.0
0.0.15.255 area172.16.16.0
QTECH(config-router)# network192.168.12.0
0.0.0.255 area 1
QTECH(config-router)# network0.0.0.0 255.255.255.255 area0
```

Related Commands

Command	Description
router ospf	Creates the OSPF routing process.

Platform Description

N/A

2.51. overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance. Use the no form of this command to restore the default setting.

overflow database *number* [hard | soft]

no overflow database

Parameter Description

Parameter	Description
<i>number</i>	Maximum number of LSAs. The range is from 1 to 4294967294.
hard soft	hard: shuts down the OSPF instance when the number of LSAs exceeds that number. soft: issues an alarm when the number of LSAs exceeds that number.

Defaults

The maximum number of LSAs supported by the current OSPF instance is not restricted by default.

Command Mode

Routing process configuration mode

Usage Guide

To shut down the OSPF instance when the number of LSAs exceeds that number, use the hard parameter; otherwise, use the soft parameter.

Configuration Examples

The following example configures that OSPF instance 10 will be shut down when there are more than 10 LSAs.

```
QTECH(config)# router ospf 10
QTECH(config-router)# overflow database 10 hard
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.52. overflow database external

Use this command to configure the maximum number of external LSAs and the waiting time from the overflow state to the normal state. Use the no form of this command to restore the default setting. overflow database external *max-dbsize wait-time*

no overflow database external

Parameter Description

Parameter	Description
<i>max-dbsize</i>	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS). The range is from 0 to 2147483647.
<i>wait-time</i>	Waiting time of the routing device from the overflow status to normal

	status. The range is from 0 to 2147483647.
--	--

Defaults

The maximum number of external-LSAs is not restricted by default.

If the maximum number of external-LSAs is restricted, the normal status cannot be restored when the maximum number is exceeded.

Command Mode

Routing process configuration mode

Usage Guide

When the number of external-LSAs exceeds the value of max-db size, the device enters the overflow state. Then no more external-LSA will be loaded and the external-LSAs generated locally will be cleared. After wait-time expires, the device restores to the normal state and external-LSAs are reloaded.

When using this function, ensure that all routers of the OSPF backbone area and common areas use the same max-db size value. Otherwise, the following situations occur:

The link status is inconsistent on the entire network and neighbors fail to achieve the Full state.

Incorrect routes occur, including loops.

AS-External-LSAs may be frequently retransmitted.

Configuration Examples

The following example configures that the maximum number of external LSAs is 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow state to the normal state is 3 seconds.

```
QTECH(config)# routerospf10
QTECH(config-router)# overflow database external10 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.53. overflow memory-lack

Use this command to allow OSPF to enter the OVERFLOW state when the memory lacks. Use the **no**

form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default

Command Mode

Routing process configuration mode

Usage Guide

The action of OSPF entering the OVERFLOW state is to discard the newly-learned external route and effectively prevent the memory from increasing.

It is possible that enabling this function causes the route loop in the whole network. To reduce that possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state.

Use the clear ip ospf process command to reset the OSPF and remove the OSPF OVERFLOW state.

Use the no form of this command to prevent the OSPF to enter the OVERFLOW state when the memory is insufficient, which may result in the constantly consumption of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.

Configuration Examples

The following example prevents the OSPF from entering the OVERFLOW state when the memory is insufficient.

```
QTECH(config)# router ospf 1
QTECH(config-router)# no overflow memory-lack
```

Related Commands

Command	Description
clear ip ospf process	Resets the OSPF instances.
show ip protocols ospf	Displays the OSPF information.

Platform Description

N/A

2.54. passive-interface

Use this command to configure the specified network interface or all interface as the passive interfaces. Use the **no** form of this command to restore the default setting.

passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ip-address* }

no passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ip-address* }

Parameter Description

Parameter	Description
<i>interface-type interface-number</i>	Interface to be set as a passive interface
default	Sets all the interfaces as passive interfaces
<i>interface-type interface-number ip-address</i>	Sets the address of the specified interface as a passive address.

Defaults

No interface is configured as a passive interface by default. All interfaces are allowed to receive or send OSPF packets.

Command Mode

Routing process configuration mode

Usage Guide

To prevent other devices in the network from dynamically learning the routing information of the device, set the specified network interface of this device as a passive interface or the IP address of the specified network interface as a passive address

Configuration Examples

The following example configures fastEthernet 0/1 as a passive interface and the IP address of the interface 1.1.1.1 as the passive address.

```
QTECH(config)# routerospf 30
QTECH(config-router)# passive-interface fastEthernet 0/1 QTECH(config-router)# passive-
interface fastEthernet 0/1 1.1.1.1
```

Related Commands

Command	Description
show ip ospf interface	Displays the configuration information of the interface.

Platform Description

N/A

2.55. redistribute

Use this command to redistribute the external routing information. Use the **no** form of this command to restore the default setting.

redistribute { bgp | connected | isis [area-tag] | ospf process-id | rip | static } [{ level-1 | level-1-2

| level-2 }] [match { internal | external [1|2] | nssa-external [1|2] }] [metric metric-value] [metric-type { 1|2 }] [route-map route-map-name] [subnets] [tag tag-value]

no redistribute { bgp | connected | isis [area-tag] | ospf process-id | rip | static } [{ level-1 | level-1-2 | level-2 }] [match { internal | external [1|2] | nssa-external [1|2] }] [metric metric-value] [metric-type { 1|2 }] [route-map route-map-name] [subnets] [tag tag-value]

Parameter Description

Parameter	Description
bgp	Redistribution from bgp

connected	Redistribution from direct routes
isis [area-tag]	Redistribution from an IS-IS instance specified in area-tag
ospf process-id	Redistribution from an ospf instance specified in process-id in the range from 1 to 65,535
rip	Redistribution from rip
static	Redistribution from static routes
level-1 level-1-2 level-2	Configures IS-IS route redistribution. The parameter specifies a level, and routes of this level will be redistributed. Only level-2 IS-IS routes can be redistributed by default.
match	Filters specified routes for configuring OSPF route redistribution. By default, all the OSPF routes are redistributed.
metric <i>metric-value</i>	Specifies the metric of an OSPF external LSA in the range from 0 to 16777214.
metric-type{1 2}	Sets the external routing type as E-1 or E-2.
route-map <i>route-map-name</i>	Redistribution filter rule
subnets	Redistributes the routes of non standard networks.
tag <i>tag-value</i>	Sets the tag value of the routes redistributed to the OSPF in the range from 0 to 4294967295.

Defaults

Redistribution configuration is not supported by default.

If you configure OSPF redistribution, all subtype routes of the instance are redistributed.

If you configure ISIS redistribution, all level-2 subtype routes of the instance are redistributed. In other cases, all routings of this type are redistributed.

The default metric of the redistribution BGP route is 1. The default metric of LSAs generated by routes of other types is 20.

The default value of metric-type is E-2. No route-map is associated by default.

Command Mode

Route configuration mode


Usage Guide

After the command is configured, the router will become an ASBR, and the related routing information is imported into the OSPF domain and broadcasted to other OSPF routers through type-5 LSAs.

When you configure is route redistribution without the level parameter, level-2 routes can be redistributed by default. In initial redistribution configuration that carries the level parameter, routes of the specified level can be redistributed. When you save the configuration containing both level 1 and level 2, they are merged into level-1-2 for convenience. For details, see the configuration examples. When you configure OSPF router distribution without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. Use the no form of this command to restore the default configuration.

When you filter routes for redistribution by following the route-map rule, the match rule of the route-map rule is specific for the original redistribution parameters. The route-map rule works only when the redistributed OSPF routes follow the match rule.

The range of set metric is from 0 to 16777214 for the associated route-map. If the value exceeds the range, introducing a route fails.

 The following are the rules for configuring the no form of the redistribute command:1. If the no

form specifies some parameters, restore their default values.2. If the no form contains no

parameter, delete the whole command. If the following configuration exists: redistribute isis 112 level-2 You can use the no redistribute isis 112 level-2command to modify the configuration.

According to preceding rules, this command restores the level-2 parameter to the default value, namely level-2. Therefore, the configuration remains the same after the no form of the preceding command is executed. redistribute isis 112 level-2 To delete the whole command, use the following command: no redistribute isis 112

Configuration Examples

The following example redistributes routes of **ospf2** and **isis** isis-001 to the OSPF area.

```
QTECH(config)# router ospf1
QTECH(config-router)# redistribute ospf 2 subnets QTECH(config-router)# redistribute
ospf2match external 1 internal
QTECH(config-router)# redistribute isisis-001
QTECH(config-router)# redistribute isisis-001 level-1
```

```
router ospf 1
redistribute ospf 2 match external 1 internal subnets redistribute isis isis-001 level-1-
```

The following example displays the output of the **show run** command.

Related Commands

Command	Description
summary-address	Configures the aggregate route for the external route of the OSPF route area.
default-metric	Sets the default metric of the OSPF redistribution route.

Platform Description

N/A

2.56. router ospf

Use this command to create the OSPF routing process in global configuration mode. Use the **no** form of this command to restore the default setting.

router ospf

router ospf *process-id* [**vrf** *vrf-name*]

no router ospf *process-id*

Parameter Description

Parameter	Description
<i>process-id</i>	ID of an OSPF process. If the process ID is not configured, process 1 is configured.
<i>vrf-name</i>	VRF of the configured OSPF process for products that support the VRF.

Defaults

No OSPF routing process exists by default.

Command Mode

Global configuration mode

Usage Guide

Based on the original implementation, the RGOS10.1 adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.

Configuration Examples

Related Commands

Platform Description

The following example creates the OSPF routing process 10 within the specified vrf: vpn_1.

```
QTECH(config)# router ospf10 vrf: vpn_1
```

Command	Description
show ip protocols	Displays the routing protocol information.
show ip ospf	Displays the OSPF information.

N/A

2.57. router ospf max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

router ospf max-concurrent-dd *number*

no router ospf max-concurrent-dd

Parameter Description

Parameter	Description
<i>number</i>	Maximum number of DD packets in the range from 1 to 65535.

Defaults

The default is 10.

Command Mode

Global configuration mode

Usage Guide

When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have (initiated or accepted) at the same time.

Configuration Examples

The following example sets the maximum number of DD packets to 4.

After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
QTECH# configure terminal
QTECH(config)# router ospfmax-concurrent-dd4
```

Related Commands

Command	Description
max-concurrent-dd	Sets the maximum number of the neighbors that the OSPF routing process can concurrently interact with.

Platform Description

N/A

2.58. router-id

Use this command to set the router ID. Use the **no** form of this command to restore the default setting.

router-id *router-id*

no router-id

Parameter Description

Parameter	Description
<i>router-id</i>	Router ID in IP address form

Defaults

The OSPF routing process will select the maximal interface IP address as the router ID by default. If the loopback interface of an IP address is not configured, the OSPF routing process will select the maximum IP address among all its physical interfaces as the router ID.

Command

Mode Routing process configuration mode

Usage Guide

You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a lot of processing. Therefore, it is not recommended to change the router ID. The device can be changed only when no LSA is generated.

Configuration Examples

The following example modifies the router ID to 0.0.0.36.

```
QTECH(config)# router ospf 20
QTECH(config-router)# router-id 0.0.0.36
```

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.

Platform Description

N/A

2.59. show ip ospf

Use this command to display the OSPF information.

show ip ospf [*process-id*]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command displays the information of the OSPF routing process.

Configuration Examples

The following example displays the output of the **show ip ospf** command.

```
QTECH# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Domain ID type 0x0105, value 0x010101010101
Process uptime is 4 minutes
Process bound to VRF default Memory Overflow is enabled.
Router is not in overflow state now.
Conforms to RFC2328, and RFC1583
Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Enable two-way-maintain
Supports opaque LSA
Supports Graceful Restart
This router is an
ASBR (injecting external routing information)
Originating router-LSAs with maximum metric
Condition:on startup for 100 seconds,
State:inactive
Advertise stub links with maximum metric in router-LSAs
Advertise summary-LSAs with metric 16711680
Advertise external-LSAs with metric 16711680
Unset reason:timer expired,
Originated for 100 seconds Unset time:00:02:02.080,
Time elapsed: 00:23:54.656
```


2. OSPFv2 Commands

161

```
SPF schedule delay 5 secs,  
Hold time between two SPF's 10 secs Initial  
LSA throttle delay 0 msec  
Minimum hold time for LSA throttle 5000 msec  
Maximum wait time for LSA throttle 5000 msec Lsa  
Transmit Pacing timer 40 msec, 10 LS-Upd  
Minimum LSA arrival 1000 msec  
Pacing lsa-group:240 secs
```

Number of incoming current DD exchange neighbors 0/5 Number of outgoing current DD exchange neighbors 0/5 Number of external LSA 4. Checksum 0x0278E0

Number of opaque AS LSA 0. Checksum 0x000000 Number of non-default external LSA 4 External LSA database is unlimited.

Number of LSA originated 6 Number of LSA received 2

Log Neighbor Adjacency Changes :Enabled Graceful-restart disabled

Graceful-restart helper support enabled Number of areas attached to this router: 1 BFD enabled

Area 0 (BACKBONE)

Number of interfaces in this area is 1(1)

Number of fully adjacent neighbors in this area is 1 Area has no authentication

SPF algorithm last executed 00:01:26.640 ago SPF algorithm executed 4 times

Number of LSA 3. Checksum 0x0204bf Area 1 (NSSA)

Number of interfaces in this area is 1(1)

Number of fully adjacent neighbors in this area is 0

Number of fully adjacent virtual neighbors through this area is 0 Area has no authentication

SPF algorithm last executed 02:09:23.040 ago SPF algorithm executed 4 times

Number of LSA 6. Checksum 0x028638

NSSA Translator State is disabled, Stability Interval expired in 00:00:03

Field	Description
Router ID	ID of a router.
Process uptime	Effective time of the current OSPF process (the process does not take effect when device-id is 0.0.0.0)
Bou to VRF	VRF of the current OSPF
Conforms to	Same as the RFC2328

RFC2328	
RFC1583Compatibility flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external routes. This policy is used in the selection of best ASBR and in the route comparison.
Support Tos	Supports Only TOS0.
Supports opaque LSA	Supports opaque-LSA.
Graceful-restart	GR Restart capability described in the RFC3623 Graceful Restart
Graceful-restart helper	GR Help capability described in the RFC3623 Graceful Restart
Router Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	Parameter used for LSA pacing, checksum calculation, and aging interval
Incoming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.

Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjacency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this router	Total number of areas on the devices
Area type	Area type, including normal, stub, and nssa

Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSATranslator State	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA.
BFD enabled	Enables BFD for OSPF.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.60. show ip ospf border-routers

Use this command to display the OSPF internal routing table on the ABR/ASBR.

show ip ospf [*process-id*] border-routers

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command displays the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the show ip route command. The OSPF internal routing table has the destination address of the router ID instead of the destination network.

Configuration Examples

The following example displays the output of the **show ip ospf border-mrouters** command.

```
QTECH# show ip ospf border-routers OSPF internal Routing Table
Codes:i - Intra-area route, I - Inter-area route
i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select
The following table describes fields in the output.
```

Field	Description
Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.
I	Intra-area routes
1.1.1.1	Displays the OSPF ID of the border device.

[2]	Displays the cost to the border device.
via 10.0.0.1	Displays the next-hop gateway to the border device.
FastEthernet 0/1	Displays the interface to the border device.
ABR, ASBR	Displays the type of the border device, including ABR, ASBR, or both.
Area 0.0.0.1	Displays the area that learns the route.
select	Indicates the currently selected optimal path when there are multiple paths to the ASBR.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.61. show ip ospf database

Use this command to display the OSPF link state database information. Use the **no** form of this command to restore the default setting. Different formats of the command will display different LSA information.

Parameter Description

show ip ospf [*process-id* [*area-id* | *ip-address*]] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }] [{ **adv-router** | **ip-address** | **self-originate** } | **link-state-id** | **brief**] [**database-summary** | **max-age** | **detail**]

Parameter	Description
area-id	(Optional) Displays the area ID.
adv-device	(Optional) Displays the LSA information generated by the specified

	advertising device.
<i>link-state-id</i>	(Optional) Displays the LSA information of the specified OSPF link state identifier.
self-originate	(Optional) Displays the LSA information generated by the device itself.
Max-age	(Optional) Displays the LSAs aged.
router	(Optional) Displays the OSPF device LSA information.
network	(Optional) Displays the OSPF network LSA information.
summary	(Optional) Displays the OSPF summary LSA information.
asbr-summary	(Optional) Displays the ASBR summary LSA information.
external	(Optional) Displays the OSPF external LSA information.
nssa-external	(Optional) Displays the category 7 OSPF external LSA information.
opaque-area	(Optional) Displays type 10 LSAs.
opaque-as	(Optional) Displays type 11 LSAs.
opaque-link	(Optional) Displays type 9 LSAs.
database-summary	(Optional) Displays the statistics of LSAs of the link state database.
detail	Displays detailed information of LSAs of the OSPF.
brief	Displays the brief information of the LSAs of the specified type.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

When the OSPF link state database is very large, you should display the information on the link state database by item. Proper use of commands may help OSPF troubleshooting.

Configuration Examples

```
QTECH# show ip ospf database
OSPF Device with ID (1.1.1.1) (Process ID 1)
Device Link States (Area 0.0.0.0)
Link ID      ADV Device    Age Seq#      CkSum Link count
1.1.1.1      1.1.1.1        2 0x80000011 0x6f39 2
3.3.3.3      3.3.3.3        120 0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID      ADV Device    Age Seq#      CkSum
```

The following example displays the output of the **show ip ospf database** command.

```
192.88.88.27 1.1.1.1        120 0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID      ADV Device    Age Seq#      CkSum Route 10.0.0.0
1.1.1.1      2            0x80000003 0x350d 10.0.0.0/24
100.0.0.0    1.1.1.1      2      0x8000000c 0x1ecb 100.0.0.0/16
Device Link States (Area 0.0.0.1 [NSSA])
Link ID      ADV Device    Age Seq#      CkSum Link count 1.1.1.1
1.1.1.1      2            0x80000001 0x91a2 1
Summary Link States (Area 0.0.0.1 [NSSA])
Link ID      ADV Device    Age Seq#      CkSum Route 100.0.0.0
1.1.1.1      2            0x80000001 0x52a4 100.0.0.0/16
192.88.88.0 1.1.1.1      2      0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID      ADV Device    Age Seq#      CkSum Route Tag 20.0.0.0
1.1.1.1      1            0x80000001 0x033c E2 20.0.0.0/24 0
100.0.0.0    1.1.1.1      1      0x80000001 0x9469 E2 100.0.0.0/280
AS External Link States
Link ID      ADV Device    Age Seq#      CkSum Route Tag
20.0.0.0    1.1.1.1      380    0x8000000a 0x7627 E2 20.0.0.0/24 0
100.0.0.0    1.1.1.1      620    0x8000000a 0x0854 E2 0
100.0.0.0/28
```

The following table describes the fields in the output of the **show ip ospf database** command.

Field	Description
OSPF Device with ID	Displays the Router ID.
Device Link States	Displays the device LSA information.
Net Link States	Displays the network LSA information.
Summary Net Link States	Displays the summary network LSA information.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
AS External Link States	Displays the type 5 autonomous external LSA information.
Link ID	Displays the Link ID.
ADV Device	Displays the ID of the device that advertises the LSAs.
Age	Displays the keepalive period of the LSA.
Seq#	Displays the sequence number of the LSA, which is used to check aged or duplicate LSAs.
Cksum	Displays the checksum of LSAs.
Link-Count	Displays the number of links in the device LSA information.
Route	Displays the device information included in the LSA.
Tag	Displays the tag of the LSA.

The following example displays the output the **show ip ospf database asbr-summary** command.

```
QTECH# show ip ospf database asbr-summary
OSPF Device with ID (1.1.1.35) (Process ID 1) ASBR-Summary
```

```

Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|-|E|-) LS Type: ASBR-
summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Device address) Advertising
Device: 1.1.1.1
LS Seq Number: 80000001 Checksum:
0xbe8c Length: 28
Network Mask: /0
TOS: 0 Metric: 1

```

The following table describes the fields in the output of the **show ip ospf database asbr-summary** command.

Field	Description
OSPF Device with ID	Displays the router ID.
AS Summary Link States	Displays the summary LSA information in the AS.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
AdvertisingRouter	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be only 0 now.

Metric	Displays the metric of the route corresponding to the LSA.
--------	--

The following example displays the output of the **show ip ospf database external** command.

```
QTECH# show ip ospf database external
OSPF Device with ID (1.1.1.35) (Process ID 1) AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|-|E|-) LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number) Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
```

```
Checksum: 0x7627 Length: 36 Network Mask: /24
Metric Type: 2 (Larger than any link state path) TOS: 0
Metric: 20
Forward Address: 0.0.0.0 External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-5 AS External Link States	Displays autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.

Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Indicates the external link type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used by other routing processes to redistribute OSPF routes.

The following example displays the output of the **show ip ospf database network** command:

```
QTECH# show ip ospf database network
OSPF Router with ID (1.1.1.1) (Process ID 1) Network Link States (Area 0.0.0.0)
LS age: 572
Options:0x2 (*|-|-|-|-|E|-) LS Type:network-LSA
```

```
Link State ID:192.88.88.27 (address of Designated Router) Advertising Router:1.1.1.1
LS Seq Number: 80000001 Checksum:0x5366 Length: 32
Network Mask: /24
Attached Router:1.1.1.1 Attached Router:3.3.3.3
```

The following table describes the fields in the output of the **show ip ospf database network** command.

Field	Description
OSPF Router with ID	Displays the router ID corresponding to the follow-up information and the process ID corresponding to the OSPF.
Network LinStates	Displays the network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Device	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the network corresponding to the LSA.
Attached Router	Displays the device that is connected with the network.

The following example displays the output of the **show ip ospf database device** command:

```
QTECH# show ip ospf database router
OSPF Router with ID (1.1.1.1) (Process ID 1) Router Link States (Area 0.0.0.0)
LS age: 322
Options:0x2 (*|---|E|) Flags:0x3 :ABR ASBR
LS Type:router-LSA Link State ID:1.1.1.1
Advertising Router:1.1.1.1 LS Seq Number: 80000012 Checksum:0x6d3a
Length: 48
Number of Links: 2
Link connected to:Stub Network
(Link ID) Network/subnet number: 100.0.1.1 (Link Data) Network Mask: 255.255.255.255
```

```
Number of TOS metrics: 0
```

TOS 0 Metric: 0

The following table describes the fields in the output of the **show ip ospf database device** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Device Link States	Displays the device LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
Flag	Flag
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Number of Links	Displays the number of links associated with the device.
Link connected to	Displays what the link is connected to and the network type.
(Link ID)	Link identifier

(Link Data)	Link data
Number of TOS metrics	TOS value, supporting TOS0 only
TOS 0 Metrics	TOS0 metric

The following example displays the output of the **show ip ospf database summary** command:

```
QTECH# show ip ospf database summary
OSPF Device with ID (1.1.1.1) (Process ID 1) Summary Link States (Area 0.0.0.0)
LS age: 499
Options: 0x2 (*|---|---|E|) LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
```

```
Advertising Device: 1.1.1.1 LS Seq Number: 80000004 Checksum: 0x330e
Length: 28 Network Mask: /24
TOS: 0 Metric: 11
```

The following table describes the fields in the output of the **show ip ospf database summary** command.

Field	Description
OSPF Router with ID	Displays the router ID.
Summary Net Link States	Displays the summary network LSA information.
LS age	Displays the keepalive period of the LSA.

Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, supporting only 0 now
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database nssa-external** command:

```
QTECH# show ip ospf database nssa-external
OSPF Device with ID (1.1.1.1) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 1
Options: 0x0 (*|-|-|-|-|-|-) LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Device: 1.1.1.1

LS Seq Number: 80000001 Checksum: 0x033c Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path) TOS: 0
Metric: 20
NSSA: Forward Address: 100.0.2.1 External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database nssa-external**

Field	Description
OSPF Router with ID	Displays the router ID.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequential number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.

NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database external** command:

```
QTECH# show ip ospf database external
OSPF Device with ID (1.1.1.1) (Process ID 1) AS External Link States
LS age: 1290
Options: 0x2 (*|---|E|) LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number) Advertising Device: 1.1.1.1
LS Seq Number: 8000000a Checksum: 0x7627 Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path) TOS: 0
Metric: 20
Forward Address: 0.0.0.0 External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-7 AS External Link States	Displays the type 7 autonomous external LSA information.

LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database database-summary**

command:

The following table describes the fields in the output of the command **show ip ospf database database-summary**.

```
QTECH# show ip ospf database database-summary OSPF process 1:
Device Link States : 4 Network Link States : 2 Summary Link States : 4 ASBR-Summary
Link States : 0 AS External Link States : 4
NSSA-external Link States: 2
```

Field	Description
OSPF Process	OSPF process ID
Router Link	Number of device LSAs in the area
Network Link	Number of network LSAs in the area
Summary Link	Number of summary LSAs in the area
ASBR-Summary Link	Number of ASBR summary LSAs in the area
AS External Link	Number of NSSA LSAs in the area
NSSA-external Link	Number of NSSA LSAs in the area

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.62. show ip ospf interface

Use this command to display the OSPF-associated interface information.

show ip ospf [*process-id*] **interface** [*interface-type interface-number*] **brief**]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID
<i>interface-type</i>	(Optional) type of the specified interface
<i>interface-number</i>	(Optional) number of the specified interface
brief	Displays the summary of the interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command displays the OSPF information on the interface.

Configuration Examples

The following example displays the output of the **show ip ospf interface fastEthernet 0/1** command:

```
QTECH# show ip ospf interface fastEthernet0/1 FastEthernet 0/1 is up, line protocol
is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500 Matching network
config: 192.88.88.0/24
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1 Transmit Delay is 1
sec, State DR, Priority 1,BFD enabled Designated Router (ID) 1.1.1.1, Interface
Address 192.88.88.27
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72 Timer intervals
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

The following table describes the fields in the output of the **show ip ospf interface serial 1/0** command.

Field	Description
FastEthernet 0/1 State	State of the network interface; UP means normal working and Down means faults.

Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router ID	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay
State	DR/BDR state ID
Priority	Priority of the interface
Designated Router(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router ID of the BRD of the interface
BDR's Interface address	Address of the BDR of the interface
Time intervals configured	Hello, Dead, Wait, and Retransmit intervals of the interface
Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of Full neighbors

Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received
DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received
Discard	Statistics on the discarded OSPF packets
BFD enabled	Enables BFD for OSPF.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.63. show ip ospf ispf

Use this command to display the ISPF calculation count in the OSPF area.

show ip ospf [*process-id*] ispf

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command displays the ISPF calculation count in the OSPF area within the last 30 minutes and total ISPF calculation count by now.

Configuration Examples

The following displays the ISPF calculation count in the OSPF area.

```
QTECH# show ip ospf 1 ispf
```

```
OSPF process 1:
Area_id      30min_counts    Total_counts
0             32             1235
1             6             356
```

Related Commands

Platform Description

Field Description:

Field	Description
Area_id	OSPF area ID.
30min_co unts	ISPF calculation count in the OSPF area within the last 30 minutes.
Total_cou nts	Total count of ISPF calculation.

Command	Description
N/A	N/A

N/A

2.64. show ip ospf neighbor

Use this command to display the OSPF neighbor list.

```
show ip ospf [ process-id ] neighbor[ statistics ] { [ interface-type interface-number ] |  
[ neighbor-id ]  
| [ detail ] }
```

Parameter Description

Parameter	Description
detail	(Optional) Displays the neighbor details.
<i>interface-type</i> <i>interface-number</i>	(Optional) Displays the neighbor information of the specified interface
<i>neighbor-id</i>	(Optional) Displays the information of the specified neighbor
statistics	(Optional) Displays the neighbor statistics.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command displays neighbor information usually used to check whether the OSPF is running normally.

Configuration Examples

The following example displays the output of the **show ip ospf neighbor** command.

```
Thread Link State Update Retransmission off  
Thread Poll Timer on  
Graceful-restart helper disabled  
BFD session state up
```

The following table describes the fields in the output of the **show ip ospf neighbor** command.

```
QTECH# show ip ospf neighbor  
OSPF process 1, 1 Neighbors, 1 is Full:
```

```

Neighbor ID  Pri      State BFD State      Dead Time      Address
3.3.3.3      1        Full/BDR Up  00:00:32      192.88.88.72
FastEthernet 0/1

QTECH# show ip ospf neighbor detail

Neighbor 3.3.3.3, interface address 192.88.88.72 In the area 0.0.0.0 via interface
FastEthernet 0/1

Neighbor priority is 1, State is Full, 11 state changes DR is 192.88.88.27, BDR is
192.88.88.72

Options is 0x52 (*|O|-|EA|-|-|E|-) Dead timer due in 00:00:32 Neighbor is up for 05:11:27
Database Summary List 0

Link State Request List 0

Link State Retransmission List 0 Crypt Sequence Number is 0 Thread Inactivity Timer on
Thread Database Description Retransmission off

Thread Link State Request Retransmission off

```

Field	Description
Neighbor ID	Neighbor ID
Pri	Neighbor priority (for selection of DR)
State	Neighbor status
Dead Time	Remaining time for the neighbor to enter the Dead status
Address	Interface address of the neighbor
Interface	Interface of the neighbor
interface address	Interface address of the neighbor device
In the area	Displays the area that learns the neighbor.
via interface	Displays the interface that learns the neighbor
Neighbor priority	Priority of the neighbor OSPF
State	OSPF neighbor connection state. FULL means the stable state; DR indicates that the neighbor is the designated device; BDR indicates that the neighbor is the backup designated device; DROTHER indicates that the neighbor is not a

	DR/BDR. Point-to-point network type has no DR or DBR.
State changes times	Times of state changes
Dead Time	Dead time of the neighbor
DR	Interface address of the DR elected by the neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected by the neighbor device (that is, the BDR field of the Hello packet)
Options	Hello packet E-bit option, where 0 indicates that the area is a STUB area; 2 indicates that the area is not a STUB area.
Dead timer due in	Dead time of the neighbor device
Neighbor up time	Period from when the device is discovered till now
Database Summary List	Statistics on the neighbor DD packets
LinkState Request List	Statistics on the neighbor LS request packets
LinkState Retransmission List	Statistics on the neighbor re-transmit packets
Crypt Sequence	

Number	Area MD5 authentication code
Thread Inactivity Timer	Status of invalid neighbor timer
Thread Database Description Retransmission	Status of DD packet timer of the interface
ThreadLinkState Request Retransmission	Status of LS request packet timer of the interface
ThreadLinkState Update Retransmission	Status of LS update packet timer of the interface
Thread Poll Timer	Poll Timer start status of the static neighbor
Graceful-restart helper	Whether it is able to function as the GR Helper of a specified neighbor

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.65. show ip ospf route

Use this command to display the OSPF routes.

show ip ospf [*process-id*] **route** [**count** | *ip-address mask*]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID. All OSPF routes will be displayed without an ID specified.
count	Statistics of various OSPF routes
<i>ip-address mask</i>	Statistics of routes which have a specified prefix and mask.

Defaults

N/A

Command Mode

Privileged mode

Usage Guide

This command displays the OSPF routing information. The count option displays the OSPF routing statistics.

Configuration Examples

The following example displays the output of the **show ip ospf route** command.

Related Commands

```
OSPF process 1:
Codes: C - connected, D - Discard , O - OSPF,
IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 0/1
C 192.88.88.0/24 [1] is directly connected, FastEthernet 0/1, Area 0.0.0.1
```

Platform Description

The following table describes the fields in the output of the **show ip ospf route** command.

Field	Description
codes	Route type and corresponding abbreviation and description
100.0.0.0/ 24	Route prefix
[1]	Route cost

via	Route next hop and interface
-----	------------------------------

Command	Description
N/A	N/A

N/A

2.66. show ip ospf spf

Use this command to display the routing count in the OSPF area.

show ip ospf [*process-id*] spf

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command displays the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.

Configuration Examples

The following example displays the output of the **show ip ospf [process-id] spf** command:

```
QTECH# show ip ospf 1 spf
```

```
OSPF process 1:
```

Related Commands

Platform Description

The following table describes the fields in the output of the **show ip ospf [process-id] spf** command.

Field	Description
Area_id	OSPF area ID
30min_counts	OSPF routing counts within the latest 30 minutes
Total_counts	Total counts of the OSPF routing till now

Command	Description
show ip ospf	Displays the OSPF summary.

N/A

2.67. show ip ospf summary-address

Use this command to display the converged route of all redistributed routes.

show ip ospf [process-id] summary-address

Parameter Description

Parameter	Description
<i>process-id</i>	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is valid only on the NSSA ABR, and displays only the routes with local aggregation operations.

Configuration Examples

The following example displays the output of the **show ip ospf summary-address** command:

```
QTECH# show ip ospf summary-address
OSPF Process 1, Summary-address:
172.16.0.0/16, Metric 20, Type 2, Tag 0, Match count 3, advertise
```

Field	Description
Summary Address	IP address to be aggregated
Summary Mask	Mask to be aggregated
Advertise	Whether to advertise the aggregated route
Status	Whether the aggregation range takes effect
Aggregated subnets	Number of external routes included in the aggregation range

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.68. show ip ospf topology

Use this command to display topology information for OSPF SPF calculation.

```
show ip ospf [ process-id [ area-id ] ] topology [ adv-router adv-router-id [ router-id ]
/ self-originate [ router-id ] ]
```

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID.
<i>area-id</i>	Displayed area ID
topology	Displays a specified OSPF process and topology information summary of an area.
adv-router	Displays topology information of a specified device. This specified device must be a directly connected neighbor of the current device.
self-originate	Displays topology information of the current device.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command helps users to understand OSPF SPF calculation topology information and troubleshoot faults caused by topology planning. If the user enables fast reroute calculation, this command displays information related to fast reroute calculation.

Configuration Examples

The following example displays the result of the show **ip ospf topology** command:

```
QTECH# show ip ospf topology
OSPF Router with ID (1.1.1.1) (Process ID 1) Router
Topology States (Area 0.0.0.0)
+1.1.1.1
  +2.2.2.2
    +4.4.4.4
  +3.3.3.3
    +4.4.4.4

+2.2.2.2
  +1.1.1.1
    +3.3.3.3
  +4.4.4.4
```

```
+3.3.3.3

+3.3.3.3
+1.1.1.1
+2.2.2.2
+4.4.4.4
+2.2.2.2
```

The following example displays the result of the **show ip ospf topology self-originate** command:

```
QTECH# show ip ospf topology self-originate OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Topology States (Area 0.0.0.0) 1.1.1.1
Self to Destination Metric: 0 Parent Node: -
Child Node:2.2.2.2 Primary next-hop: - Backup next-hop: - Backup Neighbor: -

2.2.2.2
Self to Destination Metric: 1 Parent Node: 1.1.1.1
Child Node:-
Primary next-hop: FastEthernet 0/1 via 10.0.0.1 Backup next-hop: FastEthernet 0/2 via
10.0.1.1 Backup Neighbor: 2.2.2.2
Neighbor to Destination Metric: 0 Neighbor to Self Metric: 10 Neighbor to Primary
Neighbor: 0
Self to Neighbor Metric: 1
```

The following example displays the result of the **show ip ospf topology self-originate** command:

The description of every field displayed by **show ip ospf topology self-originate** is as follows:

Field	Description
Self to Destination Metric	Metric from the root node to the current destination node
Parent Node	Parent node of the current destination node
Child Node	Child node of the current destination node
Primary next-hop	Primary next hop for reaching the current the destination node

Backup next-hop	Backup next hop for reaching the current the destination node
-----------------	---

Backup Neighbor	Backup neighbor for reaching the current the destination node
Neighbor to Destination Metric	Metric from the backup neighbor to the current destination node
Neighbor to Self Metric	Metric from the backup neighbor to the root node
Neighbor to Primary Neighbor	Metric from the backup neighbor to the primary neighbor
Self to Neighbor Metric	Metric from the root node to the backup neighbor

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.69. show ip ospf virtual-link

Use this command to display the OSPF virtual link information.

show ip ospf [*process-id*] **virtual-link** [*ip-address*]

Parameter Description

Parameter	Description
<i>process-id</i>	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.
<i>ip-address</i>	Associated ID of a virtual link neighbor

Defaults

N/A

Command Mode**Privileged EXEC mode****Usage Guide**

If no virtual link is configured, the command displays the neighbor status and other related information. The `show ip ospf neighbor` command does not display the neighbor of the virtual link.

Configuration Examples

The following is the output of the **show ip ospf virtual-links** command:

```
QTECH# show ip ospf virtual-links
Virtual Link VLINK0 to device 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 0/1 Local address
10.0.0.37/32
Remote address 10.0.0.27/32
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in
00:00:05
Adjacency state Full
```

Related Commands**Platform Description**

The following table describes the fields in the output.

Field	Description
Virtual Link VLINK0 to router	Displays the virtual link neighbors and their status.
Virtual Link State	Displays the virtual link state.
Transit area	Displays the transit area of the virtual link.
via interface	Displays the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Displays the transmit delay of the virtual link.
State	Interface state

Time intervals configured	Hello, Dead, Wait, and Retransmit interval of the interface
Adjacency State	Neighbor state, where FULL means the stable state

Command	Description
N/A	N/A

N/A

2.70. summary-address

Use this command to configure the aggregate route out of the OSPF routing domain. Use the **no** form of this command to restore the remove the aggregate route.

summary-address *ip-address net-mask* [**not-advertise** | **tag value** | **cost cost**]

no summary-address *ip-address net-mask* [**not-advertise** | **tag** | **cost**]

Parameter Description

Parameter	Description
<i>ip address</i>	IP address of the aggregate route
<i>net-mask</i>	Network mask of the aggregate route
not-advertise	Does not advertise the aggregate route. If the parameter is not configured, the aggregate route is advertised.
tag value	Sets the tag value of an aggregate route. The range is from 0 to 4,294,967,295.
cost cost	Cost value of the aggregate route. The range is from 0 to 16,777,214.

Defaults

No aggregate route is configured by default.

Command

Mode Routing process configuration mode

Usage Guide

When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in external LSAs. If the incoming routes are continuous addresses, the autonomous border device can advertise only one aggregate route, reducing the scale of routing table greatly.

Unlike the **area range** command, the **area range** command aggregates inter-OSPF-area routes, while the **summary-address** command aggregates external routes of the OSPF routing domain. For the NSSA, the **summary-address** command is valid only on the NSSA ABR now, and aggregates only redistributed routes.

Configuration Examples

The following example generates an external aggregate route 100.100.0.0/16.

```
QTECH(config)# router ospf20
QTECH(config-router)# summary-address 100.100.0.0 255.255.0.0
QTECH(config-router)# redistribute static subnets
QTECH(config-router)# network 200.2.2.0 0.0.0.255 area 1
QTECH(config-router)# network 172.16.24.0 0.0.0.255 area 0
QTECH(config-router)# area nssa
```

Related Commands

Command	Description
area-range	Configures route convergence on the OSPF area border device.
redistribute	Redistributes routes of other routing processes.

Platform Description

N/A

2.71. timers lsa arrival

Use this command to configure the time delay for the same LSA received. Use the no form of this command to restore the default setting.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

Parameter	Description
-----------	-------------

<i>arrival-time</i>	Configures the time delay when receiving the same LSA. The range is from 0 to 600000 in the unit of milliseconds.
---------------------	---

Defaults

The default is 1000.

Command Mode

Routing process configuration mode

Usage Guide

No action is done when the same LSA is received within the specified time.

Configuration Examples

The following example configures the time delay for the same LSA as 2seconds.

```
QTECH(config)# routerospf1
QTECH(config-router)# timers arrival-time 2000
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description

N/A

2.72. timers pacing lsa-group

Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for the aged link state. Use the **no** form of this command to restore the default setting. **timers pacing lsa-group seconds**

no timers pacing lsa-group

Parameter Description

Parameter	Description
<i>seconds</i>	Parameter used for LSA pacing, checksum calculation, and aging interval. The range is from 10 to 1800 in the unit of seconds.

Defaults

The default is 30.

Command Mode

Routing process configuration mode

Usage Guide

Each LSA has its own update and aging time (LSA age). If you update and age LSAs separately, many CPU resources will be consumed. To effectively use CPU resources, you can update LSAs of a device in batches.

You can use this command to modify the value of seconds, whose default value is 240 seconds. This parameter needs not to be adjusted often. The optimal group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better.

Configuration Examples

The following example configures the pacing time as 120 seconds.

```
QTECH(config)# deviceospf 20
QTECH (config-router)# timers paing lsa-group 120
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description

N/A

2.73. timers pacing lsa-transmit

Use this command to transmit the LSA grouping updating. Use the **no** form of this command to restore the default setting.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

Parameter	Description
-----------	-------------

<i>transmit-time</i>	Configures the interval of sending the LSA grouping. The range is from 10 to 1000.
<i>transmit-count</i>	Configures the number of LS-UPD packets per group. The range is from 1 to 200.

Defaults

The default configurations are as follows: Transmit-time: 40 milliseconds.
Transmit-count: 1

Command Mode

Routing process configuration mode

Usage Guide

If there are a large number of LSAs and the load on the system is heavy, you can properly use the **transmit-time** and **transmit-count** to inhibit the flooding LS-UPD packet number in the network. If the CPU and network bandwidth loads are not too much, reduce **transimi-time** and increase **transimit-count** to quicken the environment convergence.

Configuration Examples

The following example sets the interval of sending the LS-UPD packets as 50ms, the packets number as 20.

```
QTECH(config)# routerospf1
QTECH(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF process information, including the router ID.

Platform Description

N/A

2.74. timers spf

Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations. Use the **no** form of this command to restore the default setting.

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter Description

Parameter	Description
<i>spf-delay</i>	Defines the SPF calculation waiting period in seconds. The range is from 0 to 2147483647. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
<i>spf-holdtime</i>	Defines the interval between two SPF calculations in seconds. The range is from 0 to 2147483647. When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.

Defaults

For the OS not supporting the timers throttle spf command, the default values are as follows: spf-delay: 5seconds;

spf-holdtime: 10 seconds.

For the OS supporting the timers throttle spf command, by default, the timers spf command takes no effect. Spf-delay depends on the default configuration of the timers throttle spf command.

Command Mode

Routing process configuration mode

Usage Guide

Smaller values of *spf-delay* and *spf-holdtime* mean that OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the router.

The configurations of the **timers spf command** and the **timers throttle spf command** may overwrite each other.

Configuration Examples

The following example configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.

```
QTECH(config)# deviceospf20
```

Related Commands

Platform Description

```
QTECH(config-router)# timersspf 3 9
```

Command	Description
show ip ospf	Displays the configuration information of the ospf.
timers throttle spf	Configures the exponential back off delay for SPF calculation. The command is recommended to replace the timers spf command because it is more powerful.

N/A

2.75. timers throttle lsa all

Use this command to configure the exponential back off algorithm for the LSA. Use the **no** form of this command to restore the default setting.

```
timers throttle lsa all delay-time hold-time max-wait-time
```

```
no timers throttle lsa all
```

Parameter Description

Parameter	Description
<i>delay-time</i>	Configures the time delay of generating the LSA first. The range is from 1 to 600000.
<i>hold-time</i>	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is from 1 to 600000.
<i>max-wait-time</i>	Configures the maximum interval of successive refreshing the LSA., which determines whether the LSA is refreshed successively. The range is from 1 to 600000

Defaults

The default configurations are as follows:

Delay-time: 0 millisecond,

Hold-time: 5000 milliseconds,

Max-wait-time: 5000 milliseconds.

Command Mode

Routing process configuration mode

Usage Guide

If high convergence performance is required for the link change, the value of delay-time can be relatively small. if you expect to reduce the CPU consumption, increase appropriately several values.

The value of hold-time cannot be smaller than that of delay-time, and the value of max-wait-time cannot be smaller than that of hold-time.

Configuration Examples

The following example configures the first delay as 10ms, hold-time as 1second and the longest delay as 5seconds.

```
QTECH(config)# routerospf1
QTECH(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf

Platform Description

N/A

2.76. timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default setting. **timers throttle route { inter-area ia-delay | ase ase-delay }**

no timers throttle route { inter-area | ase }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
<i>ia-delay</i>	Sets the delay time of the inter-area route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the ia-delay time runs out.
ase	Calculates the external routes.
<i>ase-delay</i>	Defines the delay time of the external route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.

Defaults

The default values are as follows:

ia-delay: 0,

ase-delay: 0,

Command Mode

Routing process configuration mode

Usage Guide

The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route

calculation and save the CPU resources, increase the delay time.

Configuration Examples

The following example sets the .delay time of the inter-area route calculation to one second.

```
QTECH(config)# router ospf 1
QTECH(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.77. timers throttle spf

Use this command to configure the topology change information for OSPF, including the delay for SPF calculation as well as the interval between two SPF calculations in routing process configuration mode. Use the **no** form of this command to restore the default setting.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
<i>spf-delay</i>	Defines the SPF calculation waiting period, in the unit of milliseconds, in the range from 1 to 600,000. After receiving the topology change, the

	OSPF routing process must wait for the specified period to start the SPF calculation.
<i>spf-holdtime</i>	Defines the interval between two SPF calculations in seconds in the range from 1 to 600,000.
<i>spf-max-waittime</i>	Defines the maximum interval between two SPF calculations, in milliseconds in the range from 1 to 60,000.

Defaults

The default configurations are as follows: spf-delay: 1000ms;

spf-holdtime: 5000ms;

spf-max-waittime: 10000ms.

Command Mode

Routing process configuration mode

Usage Guide

The spf-delay parameter indicates the delay time of the topology change to the SPF calculation.

The spf-holdtime parameter indicates the minimum interval between two SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval until it reaches to

spf-max-waittime. If the interval between two SPF calculations has exceeded the required value, the

SPF calculation will restart from spf-holdtime.

Smaller spf-delay and spf-holdtime values can make the topology converge faster. A greater spf-max-waittime value can reduce the system resource consumption of SPF calculation. Those configurations can be flexibly adjusted according to the actual stability of the network topology.

Compared with the timers spf command, this command is more flexible. It speeds up the SPF calculation convergence, and reduces the system resource consumption of SPF calculation due to the topology change. To this end, the timers throttle spf command is recommended.

The value of spf-holdtime cannot be smaller than the value of spf-delay, or the value of spf-holdtime will be set to be equal to the value of spf-delay;

The value of spf-max-waittime cannot be smaller than the value of spf-holdtime, or the value of spf-max-waittime will be set to be equal to the value of spf-holdtime automatically;

The configurations of the `timers spf` command and the `timers throttle spf` command may overwrite each other.

If both the `timers spf` command and the `timers throttle spf` command are not configured, the default value of the `timers throttle spf` command is used.

Configuration Examples

The following example configures the delay and holdtime and the maximum time interval of the OSPF as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculation intervals are: 5ms, 1second, 3 seconds, 7 seconds, 15 seconds, 31 seconds, 63 seconds,

89 seconds, 179 seconds, 179+90seconds...

```
QTECH(config)# routerospf20
```

```
QTECH(config-router)# timersspf 5 1000 90000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of OSPF
timers spf	Configures the SPF calculation delay. This command is supported in versions earlier than OS 10.4. It is recommended to replace the <code>timers spf</code> command with the <code>timers throttle spf</code> command.

Platform Description

N/A

2.78. two-way-maintain

Use this command to enable the OSPF two-way-maintain function. Use the `no` form of this command to disable this function.

`two-way-maintain` `no two-way-maintain`

Parameter Description

Parameter	Description
-----------	-------------

N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

In the large-scale network, partial packets delay or dropped may exist due to much CPU and memory are occupied caused by lots of packet transmission. If the Hello packets are handled over

dead-interval, the corresponding adjacency will be disconnected. In this case, you can enable the two-way-maintain function for the packets such as DD, LSU, LSR and LSAck packets from a neighbor in the network (except for the Hello packets), avoiding the neighbor invalidation caused by delayed or dropped Hello packets.

Configuration Examples

The following example disables the OSPF two-way-maintain function.

```
QTECH(config)# routerospf1
QTECH(config-router)# notwo-way-maintain
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the OSPF

Platform Description

N/A

3. OSPFV3 COMMANDS

3.1. area authentication

Use this command to configure OSPFv3 area authentication. Use the **no** form of this command to restore the default setting.

area *area-id* **authentication ipsec spi** *spi* [**md5** | **sha1**] [**0** | **7**] *key*

no area *area-id* **authentication**

Parameter Description

Parameter	Description
<i>area-id</i>	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
md5	Specifies a message digest 5 (MD5) authentication mode.
sha1	Specifies a secure hash algorithm 1 (SHA1) authentication mode.
0	Indicates that a key is displayed in a plain-text format.
7	Indicates that a key is displayed in a cipher-text format.
<i>key</i>	Specifies an authentication key.

Defaults

Authentication is not performed by default.

Command Mode

Routing process configuration mode

Usage Guide

OS supports three authentication modes:

null authentication mode, which is configured when authentication is not needed

MD5 authentication mode

SHA1 authentication mode

If OSPFv3 area authentication is configured, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Interface authentication configuration, however, takes precedence over area authentication configuration.

Configuration Examples

The following example specifies MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
QTECH(config-router)# area 1 authentication ipsec spi 300 md5
Aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf authentication	Specifies interface authentication.
area virtual-link authentication	Specifies virtual link authentication.

Platform Description

N/A

3.2. area default-cost

Use this command to set the cost of the default route for the ABR in the stub/NSSA area. Use the **no**

form of this command to restore the default setting.

area area-id default-cost cost

no area area-id authentication

Parameter Description

Parameter	Description
<i>area-id</i>	Area ID of the stub/NSSA area. It can be an integer or an IPv4 prefix.
<i>cost</i>	Cost of the default route of the stub/NSSA area in the range from 0 to 16777215.

Defaults

The default cost is 1.

Command Mode

Routing process configuration mode.

Usage Guide

This command can only work in the ABR connected to the stub area.

Configuration Examples

The following example sets the cost of the default route of stub/NSSA area 50 to 100.

```
ipv6 router ospf 1 area 50 stub  
area 50 default-cost 100
```

Related Commands

Command	Description
area stub	Sets a stub area.

Platform Description

N/A

3.3. area encryption

Use this command to enable encryption authentication for an OSPFv3 area. Use the no form of this command to restore the default setting.

Parameter Description

area *area-id* encryption ipsec spi *spi* esp null [md5 | sha1] [0 | 7] key
no area *area-id* encryption

Parameter	Description
<i>area-id</i>	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
<i>spi</i>	Specifies a security parameter index, in the range from 256 to

	4294967295.
null	Specifies the null encryption mode.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
<i>Key</i>	Specifies an authentication key.

Defaults

Encryption authentication is not performed by default.

Command Mode

Routing process configuration mode

Usage Guide

OS supports the null encryption mode and two authentication modes: MD5 and SHA1. If encryption authentication is configured for an OSPFv3 area, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Encryption authentication configuration on interfaces, however, takes precedence over that of the OSPFv3 area.

Configuration Examples

The following example specifies null encryption and MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
QTECH(config-router)# area 1 encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf encryption	Specifies interface encryption authentication.

area virtual-link encryption	Specifies virtual link encryption authentication.
-------------------------------------	---

Platform Description

N/A

3.4. area nssa

Use this command to configure an NSSA area. Use the **no** form of this command to remove the

Parameter Description

NSSA area configuration.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [*metric value*] [*metric-type type*]] [**no-summary**] [**translator** [*stability-interval seconds* | **always**]]

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [*metric*] [*metric-type*]] [**no-summary**] [**translator** [*stability-interval* | **always**]]

Parameter	Description
<i>area-id</i>	ID of the NSSA area.
no-redistribution	(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal areas, but not into the NSSA area.
default-information-originate	(Optional) Used to generate a Type 7 default into the NSSA area. This keyword takes effect only on the NSSA ABR or the NSSA Autonomous System Boundary Router (ASBR).
metric <i>value</i>	(Optional) Specifies the OSPF default LSA metric. The range is from 0 to 16,777,214, and the default value is 1.
metric-type <i>type</i>	(Optional) Specifies the OSPF metric type for default routes. The value can be 1 or 2 and the default value is 2.
no-summary	(Optional) Allows an area to be an NSSA but not have summary routes injected into it.

translator	(Optional) Configures the NSSA ABR translator.
stability-interval <i>seconds</i>	(Optional) Configures the stability interval after the role of an NSSA ABR is changed from translator to non-translator. The range is from 0 to 2,147,483,647, the default value is 40 and the unit is second.
always	(Optional) Configures the NSSA ABR to be always translator. The default NSSA ABR is a non-translator.

Defaults

No NSSA area is defined by default.

Command

Mode Routing process configuration mode

Usage Guide

The default-information-originate parameter is used to generate a default Type 7 LSA. There is a small difference between NSSA ABR and NSSA ASBR on which this command can take effect. On the ABR, the Type-7 default route generates no matter whether a default route exists in the routing table, while on the ASBR, the Type-7 default route generates only when a default routes exists in the routing table.

The no-redistribution parameter is used when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal areas, but not into the NSSA area. This parameter is generally used on the device acting as both ASBR and ABR in NSSA area to prevent the routes from being imported into the NSSA area.

The no-summary parameter allows an area to be an NSSA but not have summary LSAs injected into it.

In an NSSA area involving two or more ABR devices, by default, the ABR of larger router ID is elected as the translator for Type-7 to Type-5 translation. You can configure the translator always parameter to specify an ABR to be always the translator.

When the translator of an ABR device is replaced, the ABR still has the translation capability within the stability-interval time. After the stability-interval timer expires and the ABR is not elected as the translator again, then the LSAs translated from Type-7 to Type-5 will be removed from the AS.

To prevent route loop, the Type-5 LSAs aggregated by the Type-7 are removed once the ABR device loses the translator capability, instead of waiting for the stability-interval expiration.

It is recommended to configure the translator always parameter on only one ABR device in an NSSA area.

Configuration Examples

The following example sets the area 1 as an NSSA area.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# area 1 nssa
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.5. area-range

Use this command to set the range of the converged inter-area addresses. Use the no form of this command to restore the default setting.

area area-id range ipv6-prefix/prefix-length [advertise|not-advertise]

no area area-id range ipv6-prefix/prefix-length

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the area in which the addresses are converged. It can be an integer or an IPv4 prefix.
<i>ipv6-prefix/prefix-length</i>	Range of the converged addresses.
advertise	Advertises the range of converged addresses.
not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.

Defaults

No converged inter-area address range is defined by default.

Command Mode

Routing process configuration mode

Usage Guide

This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. The routing information combination only takes place on the area border. The specific routing information is seen on the intra-area routers, but only one converged route can be seen on the devices in other areas. By configuring the two options of advertise and not-advertise, you can decide whether to advertise the convergence range to enable blocking and filtering. By default, the range is advertised to the outside. The option cost can be used to set the metric value of convergence routing.

A number of route convergence commands can be defined. In this way, the number of the routes in the OSPF AS is reduced. Particularly for a large network, the forwarding performance will be improved.

When a number of routes are converged, and the containment relationship exists between items, the area range converged is determined by the longest match principle.

Configuration Examples

The following example converges the routes in area 1.

```
ipv6 router ospf 1
area 1 range 2001:abcd:1:2::/64
```

Related Commands

Command	Description
summary-prefix	Sets the range of the external routes to be converged.

Platform Description

N/A

3.6. area stub

Use this command to create a stub area or set its attributes. Use the **no** form of this command to restore the default setting.

area area-id stub [no-summary]

no area area-id stub [no-summary]

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the stub area. It can be an integer or an IPv6 prefix.
no-summary	This option applies only to the ABR in the stub area, indicating that the ABR only advertises the type 3 LSA indicating the default route to the stub area, not other type 3 LSAs.

Defaults

No stub area is defined by default.

Command Mode

Routing process configuration mode

Usage Guide

If an area is at the end of an entire network, it can be designed as the stub area, in which all the routers must execute the area stub command. If the area is designed as the stub area, it cannot learn the AS external routing information (type 5 LSAs). In practical application, the external routing information takes a large proportion of the link state database, so the devices in the stub area can only learn very little routing information, thus reducing the system resources required for the running of the OSPFv3 protocol.

By default, a type 3 LSA advertisement indicating default routing on the ABR in the stub area is generated, then the devices in the stub area can get to the outside of the AS.

If a totally stub area needs to be configured, just select the keyword **no-summary** when executing the

area stub command on the ABR.

Configuration Examples

The following example enables the ABR in stub area 10 to advertise the default route to the stub area.

```
ipv6 router ospf 1 area 10 stub
area 10 stub no-summary
```

Related Commands

Command	Description
area default-cost	Sets the cost of the default route in the stub

	area.
--	-------

Platform Description

N/A

3.7. area virtual-link



Use this command to create a virtual link or set its parameters. Use the **no** form of this command to restore the default setting.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*] [**authentication ipsec spi** *spi* [**md5** | **sha1**] [**0** | **7**] *key*] [**encryption ipsec spi** *spi* **esp** **null** [**md5** | **sha1**] [**0** | **7**] *key*]

no area *area-id* **virtual-link** *router-id* [**hello-interval**] [**dead-interval**] [**retransmit-interval**] [**transmit-delay**] [**instance**] [**authentication**] [**encryption**]

Parameter Description

Parameter	Description
area-id	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
Router-id	Neighbor router ID of the virtual link.
hello-interval seconds	Sets the interval to send the hello message on the local virtual link interface in the range from 1 to 65535 in the unit of seconds.
dead-interval seconds	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. It is in the range from 1 to 65535 in the unit of seconds.
retransmit-interval seconds	Interval for retransmitting LSA on the local interface of the virtual link . The range is from 1 to 65535 in the unit of seconds.

transmit-delay <i>seconds</i>	<p>Delay on the local interface of the virtual link in sending LSA.</p> <p>The range is from 1 to 65535 in the unit of seconds.</p>
instnace <i>instance-id</i>	<p>Specifies the instance corresponding to the virtual link. No virtual link can be established between different instances.</p> <p>Range: 0.-255</p>
authentication ipsec spi <i>spi</i> [md5 sha1] [0 7] <i>key</i>	<p>Specifies OSPFv3 authentication.</p> <hr/> <p> Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format.</p> <hr/> <p><i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295.</p> <p>md5 specifies the MD5 authentication mode.</p> <p>sha1 specifies the SHA1 authentication mode.</p> <p>0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. <i>key</i> specifies an authentication key.</p>
encryption ipsec spi <i>spi esp null</i> [md5 sha1] [0 7] <i>key</i>	<p>Specifies OSPFv3 encryption authentication.</p> <hr/> <p> Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format.</p> <hr/> <p><i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295.</p> <p>null specifies the null encryption mode.</p> <p>md5 specifies the MD5 authentication mode.</p> <p>sha1 specifies the SHA1 authentication mode.</p> <p>0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is</p>

	<p>displayed in the cipher-text format.</p> <p><i>key</i> specifies an authentication key.</p>
<pre>authentication ipsec spi spi [md5 sha1] [0 7] key</pre>	<p>Specifies OSPFv3 authentication.</p> <hr/> <p>i Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format.</p> <p><i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295.</p> <p><i>md5</i> specifies the MD5 authentication mode.</p> <p><i>sha1</i> specifies the SHA1 authentication mode.</p> <p>0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format.</p>
	<p><i>key</i> specifies an authentication key.</p>

Defaults

No virtual link is defined by default

hello-interval: 10 seconds;

dead-interval: four times of the hello-interval; retransmit-interval: five seconds;

transmit-interval: one second.

Authentication and encryption are not performed by default.

Command Mode

Routing process configuration mode

Usage Guide In the OSPFv3 AS, all the areas must be connected with the backbone area to ensure that they can learn the routes of the whole OSPFv3 AS. If an area cannot be directly connected with the backbone area, it can connect it through a virtual link.

The virtual link shall not be in the stub/NSSA area

dead-interval, dead-interval and instance shall be configured consistently on both sides of the virtual link neighbors, otherwise neighboring relationship cannot be set up between the virtual neighbors.

Configuration Examples

The following example configures a virtual link.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# area 1 virtual-link 192.1.1.1
```

Related Commands

Command	Description
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
show ipv6 ospf virtual-links	Displays the OSPFv3 virtual link information.

Platform Description

N/A

3.8. auto-cost

The metric of the OSPFv3 protocol is the interface-based bandwidth. Use this command to enable the bandwidth-based interface metric calculation or modify the reference bandwidth. Use the **no** form of this command to restore the default setting.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
-----------	-------------

reference-bandwidth <i>ref-bw</i>	Reference bandwidth in the range from 1 to 4294967 Mbps.
---	--

Defaults

The interface metric is calculated based on the reference bandwidth, which is 100Mbps.

Command Mode

Routing process configuration mode

Usage Guide

Use **no auto-cost reference-bandwidth** to restore it to the default reference bandwidth.

You can use **ipv6 ospf cost** in the interface configuration mode to set the cost of the specified interface, and it takes precedence over the metric calculated based on the reference bandwidth.

Configuration Examples

The following example changes the reference bandwidth to 10M.

```
ipv6 router ospf 1
auto-cost reference-bandwidth 5
```

Related Commands

Command	Description
ipv6 ospf cost	Sets the cost of an interface.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description

N/A

3.9. bdf all-interfaces

Use this command to enable the BDF on all OSPFv3 interfaces. Use this command to enable the BDF on all OSPFv3 interfaces in the routing configuration mode. Use the **no** form of this command to restore the default setting.

bdf all-interfaces

no bdf all-interfaces

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Routing process configuration mode.

Usage Guide

The OSPFv3 protocol dynamically discovers the neighbors through the Hello packets. With the BFD function enabled, BFD sessions will be established for the neighbors that match the FULL rules and the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPFv3 will perform the network convergence immediately.

You can also use the interface configuration mode command **ipv6 ospf bfd [disable]** to enable or disable the BFD function on the specified interface, which takes precedence over the command **bfd all-interfaces** in the routing process configuration mode.

Configuration Examples

Related Commands

Platform Description

N/A

Command	Description
ipv6 router ospf <i>process-id</i>	Enables the OSPFv3 routing process and enter into the routing process configuration mode.
ipv6 ospf bfd [disable]	Enables or disable the BFD on the specified OSPFv3 interfaces.

N/A

3.10. clear ipv6 ospf process

Use this command to clear and restart the OSPF process.

clear ipv6 ospf { **process** | *process-id* }

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID, in the range from 1 to 65535

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

In normal case, it is not necessary to use this command.

Use the parameter *process-id* to clear only one specific OSPFv3 instance. If no *process-id* is specified, all the OSPFv3 instances will be cleared.

Configuration Examples

The following example restarts the OSPF process.

```
enable
clear ipv6 ospf process
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.11. default-information originate

Use this command to generate a default route to the OSPFv3 routing domain in the routing process mode. Use the no form of this command to restore the default setting.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map*]

Parameter	Description
always	(Optional) It makes OSPFv3 generate the default route unconditionally, no matter whether the default route exists locally or not.
metric <i>metric</i>	(Optional) Initial metric value of the default route, in the range from 0 to 16777214
metric-type <i>type</i>	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric seen on different routers.
route-map <i>map</i>	Associated route-map name, no associated route-map by default

Defaults

No default route is created;

The initial metric value is 1; The default route type is type 2.

Command Mode

Routing process configuration mode

Usage Guide

When the redistribute or default-information command is executed, the OSPFv3-enabled router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate the default route automatically or advertise it to all the routers in the OSPFv3 routing domain. The ASBR generates default routes by default. It is required to configure with the routing process configuration command default-information originate.

If the always parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route in the core routing table exists or not. However, the local router does not display the default route. To make sure whether the default route is generated, execute show ipv6 ospf database to observe the OSPF link state database. The execution of the show ipv6 route command on the OSPF neighbor will display the default route.

The metric of the external default route can be defined only with the default-information originate

command and cannot be set with the default-metric command.

There are two types of OSPFv3 external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes

precedence over type 2. As a result, the `show ipv6 route` command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area. To generate a default route in the NSSA area, use the `area nssa default-information-originate` command.

Configuration Examples

The following example generates a default route.

```
QTECH(config)# ipv6 router ospf 1
```

```
QTECH(config-router)# default-information originate always
```

Related Commands

Command	Description
redistribute	Redistribute routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

Platform Description

N/A

3.12. default-metric

Use this command to set the default metric for the routes to be redistributed. Use the **no** form of this command to restore the default setting

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
<i>metric-value</i>	Default metric for the routes to be redistributed. Its range is from 1 to 16777214.

Defaults

The default is 20.

Command Mode

The default route type is type 2.

Usage Guide

This command can be used together with **redistribute** to set the default metric for the routes to be redistributed. But this command does not apply to two types of routes:

The **default route generated** with default-information originate;

The redistributed direct route, for which 20 is always the default metric value.

Configuration Examples

The following example sets the default metric for the routes to be redistributed to 10.

Related Commands

Command	Description
redistribute	Redistributes the routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description

N/A

3.13. distance

Use this command to set the management distance corresponding to different types of OSPFv3 routes. Use the **no** form of this command to restore the default setting.

distance { *distance* | **ospf** { **intra-area** *distance* | **inter-area** *distance* | **external** *distance* } }

no distance [ospf]

Parameter Description

Parameter	Description
<i>distance</i>	Sets the management distance of the route, in the range from 1 to 255.
intra-area <i>distance</i>	Sets the management distance of the intra-area route, in the range from 1 to 255.

inter-area <i>distance</i>	Sets the management distance of the inter-area route, in the range from 1 to 255.
external <i>distance</i>	Sets the management distance of the external route, in the range from 1 to 255.

Defaults

The default value is 110.

Management distance of the intra-area route :110, Management distance of the inter-area route :110 Management distance of the external-area route: 110.

Command Mode

Routing process configuration mode.

Usage Guide

This command is used to specify different management distances for different types of OSPFv3 routes. The management distance of the route is used for the comparison of routing priority, the smaller the management distance is, the higher the routing priority.

The priority of the route generated by different OSPFv3 processes must be compared using the management distance. Setting the management distance as 255 indicates the routing entry is unreliable and will not for the packet forwarding.

Configuration Examples

the following example sets the OSPFv3 external route management distance to 160.

```
QTECH(config)# ipv6 router ospf 20
QTECH(config-router)# distance ospf external 160
```

Related Commands

Command	Description
ipv6 router ospf	Enables the OSPFv3 routing process .

Platform Description

N/A

3.14. distribute-list in

Use this command to filter routes that are computed based on Link State Advertisement (LSA). Use the **no** form of this command to restore the default setting.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type* *interface-number*]

Parameter Description

Parameter	Description
<i>name</i>	Specifies an ACL filtering rule.
prefix-list <i>prefix-list-name</i>	Specifies a prefix list filtering rule.
<i>interface-type</i> <i>interface-number</i>	Specifies an interface on which LSA-based routes are filtered.

Defaults

Routes are not filtered by default.

Command Mode

Routing process configuration mode

Usage Guide

Filter the routes computed based on LSA. Only the routes meeting filtering conditions can be forwarded. Route filtering does not affect the link state database and the routing tables of the neighbors. The ACL and prefix list filtering rules cannot be set at the same time. You can set only the ACL filtering rule or the prefix list filtering rule for a specific interface.

The routing filtering rules affect only forwarding of local routes but not route computation based on LSA. When route filtering is configured on an ABR, LSA can still compute routes and generate and send inter-area LSAs with prefixes to other areas. This will cause blackhole routes. To prevent the

generation of blackhole routes, you can run the **area range** command with the **not-advertise**

keyword.

Configuration Examples

The following example filters routes that are computed based on Link State Advertisement (LSA).

```
QTECH(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64
QTECH(config)# ipv6 router ospf 25
QTECH(config-router)# redistribute rip metric 100
QTECH(config-router)# distribute-list prefix-list aaa in ethernet 0/1
```

Related Commands

Command	Description
area range	Configures route aggregation in an area.

Platform Description

N/A

3.15. distribute-list out

Use this command to filter routes that are re-distributed. This command has the similar function as the

redistribute command. Use the **no** form of this command to restore the default setting.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*]] **ospf**

process-id | **rip** | **static**]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*]] **ospf**

process-id | **rip** | **static**]

Parameter Description

Parameter	Description
<i>name</i>	Specifies the ACL filtering rule.
prefix-list <i>prefix-list-name</i>	Specifies the prefix list filtering rule.
bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static	Specifies the source from which the routes are filtered.

Defaults

Routes are not filtered by default.

Command Mode

Routing process configuration mode

Usage Guide

The **distribute-list out** command has the similar function as the **redistribute route-map** command.

It can be used to filter the routes that are re-distributed based on other protocols into an OSPFv3 area. It does not directly re-distribute routes but works with the **redistribute** command to re-distribute routes. The ACL and prefix list filtering rules cannot be configured at the same time. You can set only the ACL filtering rule or the prefix list filtering rule to filter the routes from a specific source.

Configuration

Examples

The following example filters static routes that are re-distributed.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# redistribute static subnets
QTECH(config-router)# distribute-list prefix-list jjj out static
```

Related Commands

Command	Description
redistribute	Re-distributes routes that are carried by other routing processes.

Platform Description

N/A

3.16. enable mib-binding

Use this command to bind MIB to a specific OSPFv3 process. Use the **no** form of this command to restore the default setting.

enable mib-binding no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults

MIB is bound to an OSPFv3 process with the smallest process number by default.

Command Mode

Routing process configuration mode

Usage Guide

OSFPv3 MIB has no configuration information about OSFPv3 processes. You can operate only one OSFPv3 process through SNMP. OSFPv3 MIB is bound to the OSFPv3 process with the smallest process number by default. Users' operations take effect on this process.

To operate a specific OSFPv3 process through SNMP, you can bind OSFPv3 MIB to the process.

Configuration Examples

The following example enables users to operate the OSPFv3 process with the process number of 100 through SNMP.

```
QTECH(config)# ipv6 router ospf 100
QTECH(config-router)# enable mib-binding
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable traps	Enables the OSPFv3 trap function.

Platform Description

N/A

3.17. enable traps

OSPFv3 processes support eight types of trap information, which are classified into two categories. Use this command to send specific trap information. Use the **no** form of this command to restore the default setting.

```
enable traps [ error [ IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket ] |
state-change [ IfStateChange | NbrStateChange | NssaTranslatorStatusChange |
VirtIfStateChange | VirtNbrStateChange ] ]
```

```
no enable traps [ error [ IfConfigError | IfRxBadPacket | VirtIfConfigError |
VirtIfRxBadPacket ] | state-change [ IfStateChange | NbrStateChange |
NssaTranslatorStatusChange | VirtIfStateChange | VirtNbrStateChange ] ]
```

Parameter Description

Parameter	Description	
Error	Configures all error-related trap types. This keyword can also specify the following types of error traps:	
	IfConfigError	Specifies an interface parameter error;
	IfRxBadPacket	Specifies incorrect packets received by an interface;
	VirtIfConfigError	Specifies a parameter error on a virtual interface;
	VirtIfRxBadPacket	Specifies incorrect packets received by a virtual interface.
state-change	Configures all traps related to state change. This keyword can also specify the following traps related to state change:	
	IfStateChange	Specifies state change of an interface;
	NbrStateChange	Specifies state change of a neighbor;
	NssaTranslatorStatusChange	Specifies status change of the NSSA translator.
	VirtIfStateChange	Specifies state change of a virtual interface;
	VirtNbrStateChange	Specifies state change of a virtual neighbor.

Defaults

All traps are disabled by default.

Command Mode

Routing process configuration mode

Usage Guide

Before configuring this command, you must run the **snmp-server enable traps ospf** command; otherwise, OSPFv3 trap information cannot be sent correctly. This is because the function of this command is restricted by the **snmp-server** command.

You can synchronously enable the trap function of different processes even if MIB is not bound to these processes.

Configuration Examples

The following example enables all traps of OSPFv3 process 100.

```
QTECH(config)#ipv6 router ospf 100
QTECH(config-router)# enable traps
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable mib-binding	Binds MIB to an OSPFv3 process.
snmp-server enable traps ospf	Enables OSPFv3 to send trap information.

Platform Description

N/A

3.18. graceful-restart

Use this command to enable the OSPFv3 graceful restart (GR) function and to set the GR period. Use the **no** form of this command to restore the default setting.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [*graceful-period*]

Parameter Description

Defaults

This function is enabled by default.

Parameter	Description
grace-period <i>grace-period</i>	Configures the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment when OSPFv3 gracefully restarts. The GR period is in the range from 1 to 1800 in the unit of seconds. The default is 120.

inconsistent-lsa-checking	Configures the topology change detection. Once the topology change is detected, the device will exit GR and finish the convergence, This function is enabled by default after GR is enabled.
----------------------------------	---

Command Mode

Routing process configuration mode

Usage Guide

GR is configured based on the OSPFv3 instance. Different instances could be configured with different parameters.

Use this command to configure the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment that OSPFv3 gracefully restarts. In this period, the device will perform link reconstruction to restore OSPFv3. When the GR period expires, OSPFv3 exits GR and finishes regular operation.

To enable the GR function and set the GR period to the 120 seconds, use the graceful-restart command. To modify the GR period, use the graceful-restart grace-period command. Topology stability is indispensable for uninterrupted forwarding. If topology changes, OSPFv3 finishes convergence instead of continuing GR to avoid long time interruption

Disabling the topology change detection: If the topology cannot converge in time in the hot backup process, the long term forwarding interruption may occur.

Enabling the topology change detection: Forwarding interruption may occur but the interruption time is much shorter than the time it takes to disable topology detection.

It is not recommended to disable the topology change detection. In some scenario where long term forwarding interruption does not occur, disabling the topology change detection minimizes the forwarding interruption time.

The GR function is unavailable when the Fast Hello function is enabled.

Configuration Examples

The following example enables GR for OSPFv3 instance 1 and sets the GR period to 60 seconds.

```
QTECH(config)# ipv6 router ospf 1 QTECH(config-
router)# graceful-restart
QTECH(config-router)# graceful-restart grace-p
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.19. graceful-restart helper

Use this command to enable the OSPFv3 graceful restart helper function. Use the **no** form of this command to disable this function.

graceful-restart helper disable

no graceful-restart helper disable

Use this command configure the topology change detection method of OSPFv3 GR helper. Use the

no form of this command to cancel the configuration.

graceful-restart helper { strict-lsa-checking | internal-lsa-checking } no graceful-restart helper {strict-lsa-checking | internal-lsa-checking }

Parameter Description

Parameter	Description
disable	Disables the device to assist other devices in performing GR.
strict-lsa-checking	Checks the change of the LSA of types 1-5 and 7 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.
internal-lsa-checking	Checks the change of the LSA of types 1–3 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.

Defaults

The GR helper is enabled by default.

The device where the GR helper is enabled does not check the LSA change by default.

Command Mode

Routing process configuration mode

Usage Guide

Use this command to enable the GR helper function. When one neighbor device performs graceful restart, the Grace-LSA is advertised to all neighbors. If the device enabled with the GR helper receives the Grace-LSA, it will become the GR Helper to help the neighbors

perform GR. The **disable** option means that it is not allowed to perform the GR helper function for any device in GR.

The GR helper does not perform the network change detection by default. The convergence is not performed again until the GR is implemented even if the network changes. Use the

strict-lsa-checking or **internal-lsa-checking** command to enable the device to detect the change of network topology during the GR. The former checks any LSA (types 1-5,7) that stands for the network information, the latter checks the LSA that stands for the AS inner-area route. In the large scale network, it is not recommended to enable the LSA check option because the partial network changes trigger the ending of the GR, decreasing the convergence speed of the entire network.

Configuration Examples

The following example disables the GF helper function of the OSPFv3 instance 1 and modifies the topology change detection policy.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# graceful-restart helper disable
QTECH(config-router)# no graceful-restart helper disable
QTECH(config-router)# graceful-restart helper strict-lsa-checking
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.20. ipv6 ospf area

Use this command to enable the interface to participate in the OSPFv3 routing process. Use the **no**

Parameter Description

form of this command to restore the default setting.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter	Description
<i>process-id</i>	OSPF process ID.

area <i>area-id</i>	OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode.

Usage Guide

You can use this command to enable the OSPFv3 on an interface, and then configure the OSPFv3 process with `ipv6 router ospf`. It will be automatically started after this command is used., it will be automatically started after this command is used.

Use `no ipv6 ospf area` to disable the specified interface to participate in the OSPFv3 routing process. Use `no ipv6 router ospf` to disable all the interfaces to participate in the OSPFv3 routing process.

The neighbor relationship can only be established between the routers with the same instance ID. After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3.

Configuration Examples

The following example starts the OSPFv3 process on int fastethernet 0/0 for the specified area of the specified instance.

```
int fastethernet 0/0
ipv6 ospf 1 area 2 instance 2
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
passive-interface	Setsthe a passive interface.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description

N/A

3.21. ipv6 ospf authentication

Use this command to configure OSPFv3 interface authentication. Use the no form of this command to restore the default setting.

```
ipv6 ospf authentication [ null | ipsec spi spi [ md5 | sha1 ] [ 0 | 7 ] key ] [ instance instance-id ]
```

```
no ipv6 ospf authentication [ instance instance-id ]
```

Parameter Description

Parameter	Description
null	Indicates that authentication is not performed.
<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
<i>key</i>	Specifies an authentication key.

Defaults

Authentication is not performed by default.

Command Mode

Interface configuration mode

Usage Guide

OS supports three authentication modes:

- null authentication mode, which is configured when authentication is not needed
- MD5 authentication mode
- SHA1 authentication mode

OSPFv3 authentication parameters configured on interconnected interfaces must be consistent

Configuration Examples

The following example specifies MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
QTECH(config-if)# ipv6 ospf authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf authentication	Specifies interface authentication.
area virtual-link authentication	Specifies virtual link authentication.

Platform Description

N/A

3.22. ipv6 ospf bfd

Use this command to enable or disable the BFD on the specified OSPFv3-enabled interface. Use the

no form of this command to restore the default setting.

ipv6 ospf bfd [disable] [instance *instance-id*]

no ipv6 ospf bfd [instance *instance-id*]

Parameter Description

Parameter	Description
disable	Disables the BFD function on the specified OSPF interface.
instance <i>instance-id</i>	Configures the specified OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

No configuration is made by default. The BFD configuration in the OSPFv3 process configuration mode will apply.

Command Mode

Interface configuration mode.

Usage Guide

The command `ipv6 ospf bfd` in the interface configuration mode takes precedence over the `bfd all-interfaces` command in the routing process configuration mode.

You can use this command to enable the BFD on the specified interface according to the actual environment, also can use the command `bfd all-interfaces` in the OSPFv3 process configuration mode to enable the BFD function on all OSPFv3 interfaces and use the command `ip v6 ospf bfd disable` to disable the BFD on the specified interface.

Configuration Examples

```
QTECH(config)# int fastethernet 0/0
QTECH(config-if-fastethernet 0/0)# ipv6 ospf bfd
```

Related Commands

Command	Description
ipv6 router ospf <i>process-id</i>	Starts the OSPFv3 routing process and enter into the routing process configuration mode.
bfd all-interfaces	Enables the BFD on all OSPFv3 interfaces.

Platform Description

N/A

3.23. ipv6 ospf cost

Use this command to set the cost of the interface. Use the `no` form of this command to restore the default setting

```
ipv6 ospf cost cost [ instance instance-id ]
```

```
no ipv6 ospf cost [ instance instance-id ]
```

Parameter	Description
<i>Cost</i>	Cost of interface, in the range from 0 to 65535.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the
	range from 0 to 255.

Defaults

The default interface cost is the reference bandwidth/Bandwidth (100Mbps by default).

Command Mode

Interface configuration mode.

Usage Guide By default, the cost of the OSPFv3 interface is 100Mbps/Bandwidth, in which the Bandwidth is the bandwidth of the interface and configured with the command bandwidth in the interface configuration mode.

The default costs of OSPFv3 interfaces for several typical lines are:

64K serial line: 1562;

E1 line: 48

10M Ethernet: 10

100M Ethernet: 1

The OSPFv3 cost configured with the command `ipv6 ospf cost` will overwrite the default configuration.

Configuration Examples

The following example sets the cost of the interface to 1:

```
QTECH(config)# int fastethernet 0/0
QTECH(config-if)# ipv6 ospf cost 1
```

Related Commands

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.

ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.
-----------------------	--

Platform Description

N/A

3.24. ipv6 ospf dead-interval

Use this command to set a dead interval of neighbors on an interface. If no hello packet is received from a neighbor within the interval, the neighboring relationship is considered to fail. Use the **no** form of this command to restore the default setting

ipv6 ospf dead-interval { *seconds* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter	Description
<i>seconds</i>	Dead interval of neighbors. Its range is from 1 to 65535 in the unit of seconds.
minimal hello-multiplier <i>multiplier</i>	Enables the fast hello function, which takes 1s as the dead interval of neighbors. <i>Multiplier</i> specifies the number of hello packets sent in one second, in the range from 3 to 20.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

If the fast hello function is not enabled, the dead interval of neighbors is four times longer than the hello interval.

If the hello interval is changed, the dead interval of neighbors varies automatically.

Command Mode

Interface configuration mode

Usage Guide

The dead interval of neighbors must be longer than the hello interval.

The OSPFv3 fast hello function allows OSPFv3 to fast discovery neighbors and detect whether neighboring relationships are valid. To enable the OSPFv3 fast hello function, you can specify the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter in this command. **minimal** specifies the deal interval of neighbors to be 1s; **hello-multiplier** specifies the number of times that hello packets are sent in a second. Therefore, this configuration reduces the hello interval to be shorter than 1s.

If an interface is enabled with the fast hello function, the **hello-interval** field of hello packets to be advertised by this interface is set to 0, and that of hello packets received from this interface is omitted.

dead-interval, **minimal**, and **hello-multiplier** that are introduced to enable the fast hello function cannot be configured together with **hello-interval**.

No matter whether the fast hello function is configured, the dead interval of neighbors on the interconnected interfaces of neighbors must be consistent. The values of **hello-multiplier** on the interconnected interfaces can be different but you must ensure that at least one hello packet is received within the dead interval of neighbors.

You can use the **show ipv6 ospf interface** command to monitor the dead interval of neighbors and the fast hello interval on an interface.

Configuration Examples

The following example sets the dead interval of neighbors to 60 seconds on an interface.

```
QTECH(config)# int fastethernet 0/0

QTECH(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
ipv6 ospf hello-interval	Sets the interval for sending the Hello message
	on an interface.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process
-----------------------	---

Platform Description

N/A

3.25. ipv6 ospf encryption

Use this command to enable OSPFv3 encryption authentication on an interface. Use the **no** form of this command to restore the default setting.

ipv6 ospf encryption [null | ipsec spi spi esp null [md5 | sha1] [0 | 7] key]

no ipv6 ospf encryption

Parameter Description

Parameter	Description
null	Indicates that encryption authentication is not performed.
<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
<i>key</i>	Specifies an authentication key.

Defaults

Encryption authentication is not performed by default.

Command Mode

Interface configuration mode

Usage Guide

OS supports the null encryption mode and two authentication modes: MD5 and SHA1.

OSPFv3 encryption authentication parameters configured on interconnected interfaces must be consistent.

Configuration Examples

The following example specifies null encryption and MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
QTECH(config-if)# ipv6 ospf encryption ipsec spi 300 esp null md5  
aaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
area encryption	Specifies area encryption authentication.
area virtual-link encryption	Specifies virtual link encryption authentication.

Platform Description

N/A

3.26. ipv6 ospf hello-interval

Use this command to set the interval for the interface to send the Hello message. Use the **no** form of this command to restore the default setting

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
<i>seconds</i>	Interval for sending the Hello message. Its range is from 1 to 65535 in the unit of seconds.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.

Defaults

The broadcast network and point-to-point network :10 seconds. The point-to-multipoint network and NBMA network :30 seconds.

Command Mode

Interface configuration mode.

Usage Guide

The same hello sending intervals must be set for the neighbors, otherwise the normal adjacency cannot be established.

The dead-interval minimal hello-multiplier and hello-interval parameters for Fast Hello cannot be configured simultaneously.

Configuration Examples

Related Commands

Platform Description

The following example sets the interval for the interface to send the Hello message to 20 seconds.

```
ipv6 ospf hello-interval 20
```

Command	Description
ipv6 ospf dead-interval	Sets the interval for the interface to consider that the neighbor fails.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3

	routing process.
--	------------------

N/A

3.27. ipv6 ospf mtu-ignore

Use this command to ignore the MTU check when an interface receives the database description message. Use the **no** form of this command to restore the default setting.

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter Description

Parameter	Description
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

The MTU check is enabled by default.

Command Mode

Interface configuration mode.

Usage Guide

After receiving the database description message, the OSPFv3 device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an MTU greater than its own interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration Examples

The following example disables the MTU check function on the ethernet 1/0.

```
QTECH(config)# interface ethernet 1/0
QTECH(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

ipv6 mtu	Sets the value of IPv6 MTU of the interface.
-----------------	--

Platform Description

N/A

3.28. ipv6 ospf neighbor

Use this command to configure the OSPFv3 neighbor manually. Use the **no** form of this command to restore the default setting.

ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [poll-interval <0-2147483647> | priority <0-255>]] [instance *instance-id*]

no ipv6 ospf neighbor *ipv6-address* [[cost <1-65535>] [**poll-interval** < 0-2147483647 > | **priority** < 0-255 >]] [**instance** *instance-id*]

Parameter Description

Parameter	Description
cost <i>cost</i>	(Optional) Configures the cost to each neighbor in point-to-multipoint network. It is not defined by default, where the cost configured on the interface will be used. It ranges from 1 to 65535. Only the networks of the point-to-multipoint type support this option.
poll-interval <i>seconds</i>	(Optional) Interval for polling the neighbors (in seconds), which ranges from 1 to 2147483647. Only the networks of the non-broadcast (NBMA) type support this option.
priority <i>priority</i>	(Optional) Configures the priority value of non-broadcast network neighbors, which ranges from 0 to 255. Only the non-broadcast (NBMA) type network supports this option.
instance <i>instance-id</i>	(Optional) Configures the specific OSPFv3 instance on the interface, which ranges from 0 to 255.

Defaults

No neighbor is defined;

Neighbor polling interval: 120 seconds;

Priority value of non-broadcast network neighbor: 0.

Command Mode

Interface configuration mode.

Usage Guide

You can set relevant parameters for the neighbors depending on the actual network type.

Configuration Examples

The following example shows how to configure the OSPFv3 neighbor in NBMA network as follows: IPv6 address: fe80::2d0:f8ff:fe22:3533, priority value: 1, polling interval: 150 seconds.

```
QTECH(config)# interface fastEthernet 0/1 QTECH(config-if)# ipv6 ospf network non-  
broadcast  
QTECH(config-if)# ipv6 ospf neighbor fe80::2d0:f8ff:fe22:3533 priority 1  
poll-interval 150
```

Related Commands

Command	Description
ipv6 ospf priority	Sets the priority value of an interface.
ipv6 ospf network	Sets the network type of an interface.

Platform Description

N/A

3.29. ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore the default setting.

Parameter Description

Parameter	Description
broadcast	Specifies the broadcast network type.

3. OSPFv3 Commands

non-broadcast	Specifies the non-broadcast network type.
point-to-point	Specifies the point-to-point network type.
point-to-multipoint	Specifies the point-to-multipoint network type.
point-to-multipoint non-broadcast	Specifies the point-to-multipoint non-broadcast network type.
instance instance-id	Configures the specific OSPFv3 instance on the interface with the valid id range from 0 to 255.

```

ipv6 ospf network { broadcast | non-broadcast | point-to-point | point-to-multipoint
[ non-broadcast ] } [ instance instance-id ]
no ipv6 ospf network [ broadcast | non-broadcast | point-to-point | point-to-multipoint
[ non-broadcast ] ] [ instance instance-id ]

```

Defaults

Point-to-point network type: PPP, SLIP, frame relay point-to-point sub-interface and X.25 point-to-point sub-interface encapsulation.

NBMA network type: frame relay(except for the point-to-point sub-interface) and X.25 encapsulation (except for the point-to-point sub-interface)

Broadcast network type: Ethernet encapsulation.

The point-to-multipoint network type is not the default type.

Command Mode

Interface configuration mode.

Usage Guide

You can set the network type of the interface according to the actual link type applied and the topology.

Configuration Examples**Related Commands****Platform Description**

The following example sets the network type of the interface that participates in the OSPFv3 to point-to-point.

```

ipv6 ospf network point-to-point

```

Command	Description
ipv6 ospf priority	Sets the interface priority.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

N/A

3.30. ipv6 ospf priority

Use this command to set the interface priority. Use the **no** form of this command to restore the default setting.

ipv6 ospf priority *number-value* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter Description

Parameter	Description
<i>number-value</i>	The priority of the interface. Its range is from 0 to 255.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface. Its range is from 0 to 255.

Defaults

The default priority is 1.

3.31. Command Mode

Interface configuration mode.

Usage Guide

In the broadcast network type, it is necessary to elect the DR/BDR. In electing the DR/BDR, the device of a higher priority is preferred. If several devices are of the same priority, the one with the largest router-ID is preferred.

The device with the priority level of 0 does not participate in the election of DR/BDR.

Configuration Examples

The following example disables the interface from being elected as the DR/BDR.

```
QTECH(config)# interface ethernet 1/0
```

```
QTECH(config-if)# ipv6 ospf priority 0
```

Related Commands

Command	Description
ipv6 ospf network	Sets the network type of an interface.
router-id	Sets the ID of a router.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.

Platform Description

N/A

3.32. ipv6 ospf retransmit-interval

Use this command to set the interval for the interface to retransmit the LSA. Use the **no** form of this

Parameter Description

command to restore the default setting.

ipv6 ospf retransmit-interval *seconds* [instance *instance-id*]

no ipv6 ospf retransmit-interval [instance *instance-id*]

Parameter	Description
<i>seconds</i>	Interval for retransmitting the LSA. Its range is from 1 to 65535 in the unit of seconds.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.

Defaults

The default is five seconds.

Command Mode

Interface configuration mode.

Usage Guide

To ensure the reliability of the routing information transmission, the LSA sent to the neighbor shall be acknowledged by the neighbor. You can use this command to set the interval for the acknowledgement by the neighbor. If no acknowledgement is received within the specified period, the LSA information will be retransmitted.

Configuration Examples

The following example sets the interval for retransmitting the LSA to 10 seconds.

Related Commands

Command	Description
<code>show ipv6 ospf interface</code>	Displays the OSPFv3 interface information.
<code>ipv6 ospf area</code>	Sets the interface to participate in the OSPFv3 routing process.

Platform Description

N/A

3.33. ipv6 ospf subvlan

Use this command to enable OSPFv3 on super VLANs. Use the **no** form of this command to restore the default settings.

`ipv6 ospf subvlan [all | vid] no ipv6 ospf subvlan`

Parameter Description

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults

The default settings take effect only on super VLANs with OSPFv3 disabled.

Command Mode

Interface configuration mode.

Usage Guide

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the OSPF function does not need to be enabled on a super VLAN. Therefore, the OSPF function is disabled by default. However, in some scenarios, the OSPF function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration Examples

The following example sends the OSPF multicast packets to sub VLAN 1024 of super VLAN 300.

```
QTECH(config)# interface vlan 300
QTECH(config-if-VLAN 300)# ipv6 ospf subvlan 1024
```

3.34. ipv6 ospf transmit-delay

Use this command to set the delay on the interface in sending the LSA. Use the no form of this command to restore the default setting.

`ipv6 ospf transmit-delay seconds [instance instance-id]`

`no ipv6 ospf transmit-delay [instance instance-id]`

Parameter Description

Parameter	Description
<i>seconds</i>	The delay in sending LSA. Its range is from 1 to 65535 in the unit of seconds.
instance <i>instance-id</i>	Configures the ID of a specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

The default is one.

Command Mode

Interface configuration mode.

Usage Guide

Use this command to set the delay on the interface in transmitting the LSA.

Configuration Examples

The following example sets the delay on the interface in transmitting the LSA.

```
QTECH(config)# interface ethernet 1/0
QTECH(config-if)# ipv6 ospf transmit-delay 2
```

Related Commands

Command	Description
<code>show ipv6 ospf interface</code>	Displays the OSPFv3 interface information.

Platform Description

3.35. ipv6 router ospf

Use this command to start the OSPFv3 routing process. Use the no form of this command to restore the default setting.

ipv6 router ospf

ipv6 router ospf *process-id* [vrf *vrf-name*]

no ipv6 router ospf *process-id*

Parameter Description

Parameter	Description
<i>process-id</i>	OSPFv3 process ID number. Without the process number configured, it indicates that process 1 is started.
<i>vrf-name</i>	Specifies the VRF that OSPFv3 process belongs to.

Defaults

No OSPFv3 routing process is started.

Command Mode

Global configuration mode.

Usage Guide

After the OSPFv3 process is started, the routing process configuration mode is entered.

At present, our products support up to 32 OSPFv3 processes.

Configuration Examples

Related Commands

The following example starts OSPFv3 process in the specified VRF VPN1.

QTECH(config)# ipv6 router ospf 1 vrf vpn_1

Command	Description
ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.

show ipv6 ospf	Displays the OSPFv3 routing process information.
----------------	--

Platform Description

N/A

3.36. ipv6 router ospf max-concurrent-dd

Use this command to set the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes. Use the **no** form of this command to restore the default setting.

ipv6 router ospf max-concurrent-dd *number*

no ipv6 router ospf max-concurrent-dd

Parameter Description

Parameter	Description
<i>number</i>	Maximum concurrent interacting neighbors, in the range from 1 to 65535.

Defaults

The default is 5.

Command Mode

Global configuration mode

Usage Guide

When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes can be restricted.

Configuration Examples

The following example sets the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
QTECH#conf terminal
QTECH(config)#ipv6 router ospf max-concurrent-dd 4
```

Related Commands

Command	Description
max-concurrent-dd	Sets the maximum concurrent interacting neighbors in the OSPFv3 processes

Platform Description

N/A

3.37. log-adj-changes

Use this command to enable the logging of adjacency changes. Use the **no** form of this command to restore the default setting.

log-adj-changes

no log-adj-changes

Parameter Description

Parameter	Description
detail	Displays details of adjacency changes

Defaults

By default, the adjacency state log on the entry of or exit from the FULL state is output.

Command Mode

Routing process configuration mode

Usage Guide

N/A

Configuration Examples

The following example turns on the log of adjacency state change.

```
QTECH(config)# router ospf 1
QTECH(config)# log-adj-changes detail
```

Related Commands

Command	Description
show ipv6 ospf	Displays the OSPF global configuration information

Platform Description

N/A

3.38. max-concurrent-dd

Use this command to set the maximum number of DD packets that can be processed concurrently in the OSPFv3 routing process. Use the **no** form of this command to restore the default setting.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description

Parameter	Description
<i>number</i>	Maximum number of DD packets that can be processed concurrently, in the range from 1 to 65535.

Defaults

The default is 5.

Command Mode

Routing process configuration mode.

Usage Guide

When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in each OSPFv3 instance can be restricted.

Configuration Examples

The following example sets the maximum concurrent interacting neighbors allowed in the current OSPFv3 routing process to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this

device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
router ipv6 ospf 1
max-concurrent-dd 4
```

Related Commands

Command	Description
ipv6 router ospf max-concurrent-dd	Sets the maximum concurrent interacting neighbors allowed in the OSPFv3 processes.

Platform Description

N/A

3.39. passive-interface

Use this command to set the passive interface. Use the **no** form of this command to restore the default setting.

passive-interface { **default** | *interface-type interface-number* }

no passive-interface { **default** | *interface-type interface-number* }

Parameter Description

Parameter	Description
default	Sets all the interfaces to passive ones.
<i>interface-type interface-number</i>	Sets the specified interface to a passive one.

Defaults

No passive interface is set by default.

Command Mode

Routing process configuration mode

Usage Guide

After an interface is set to a passive one, it no longer receives or sends the hello message.

This command applies to the interfaces participating in the OSPFv3 but not to the virtual links.

Configuration Examples

The following example enables only the VLAN1 interface to participate in the OSPFv3 process.

```
passive-interface default
no passive-interface vlan 1
```

Related Commands

Command	Description
ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.

Platform Description

N/A

3.40. redistribute

Use this command to start the route redistribution in order to import the routing information of other routing protocols to the OSPFv3 routing process. Use the no form of this command to restore the default setting.

```
redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | rip | static } [ { level-1 | level-1-2 } | match { internal | external [1|2] | nssa-external [ 1 | 2 ] } | metric metric-value | metric-type {1|2} | route-map route-map-name / tag tag-value ]
no redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | rip | static } [ { level-1 | level-1-2 | level-2 } | match { internal | external [1|2] | nssa-external [ 1 | 2 ] } | metric | metric-type { 1|2 } | route-map route-map-name / tag tag-value ]
```

Parameter	Description
bgp	The bgp protocol is redistributed.
connected	The directly connected route is redistributed.
isis[area-tag]	The isis is redistributed. The area-tag specifies a particular isis instance.
ospf process-id	The ospf is redistributed. The process-id specifies a particular ospf instance within the range of 1-65535.
rip	The rip is redistributed.
static	The static route is redistributed.
level-1 level-1-2 level-2	It is used in the IS-IS route redistribution only and redistributes the routes at a specified level. .

match	It is used in the OSPFv3 route redistribution only and filters specific routes for redistribution;
	internal: inter-area and intra-area routes. external [1 2]: E1, E2 or all external routes. Nssa-external [1 2]: N1, N2 or all external routes of the NSSA area. All sub-type OSPFv3 routes are redistributed by default.
metric <i>metric-value</i>	Specifies the metric for the OSPFv3 external 2 LSA with metric-value. Its range is 0 to 16777214.
metric-type { 1 2 }	Set the metric type for the external route to E-1 or E-2.
route-map <i>map-map-name</i>	Specifies the routing policy for route redistribution. The name of map-tag can be composed of up to 32 characters. No route-map is associated by default.
tag <i>tag-value</i>	Specifies the tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.

Defaults

The function is disabled by default;

Metric-type: 2;

Level-2 routes are redistributed in the ISIS redistribution

OSPFv3 routes of all sub-types are redistributed in the OSPFv3 redistribution No route-map is associated

Command Mode

Routing process configuration mode

Usage Guide

When a device supports multiple routing protocols, the coordination between these protocols becomes an important task. The device can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

The parameters *level-1*, *level-2* or *level-1-2* can be configured in the redistribution of the ISIS routes to indicate the level of the routes in the redistribution. By default, the *level-2* ISIS routes are redistributed

When redistributing OSPFv3 routes, you can configure *match* to redistribute the routes of the corresponding sub-type among the redistributed OSPFv3 routes. All types of OSPFv3 routes are redistributed by default.

The *match* parameter of route-map is specific to the source of routes. The parameters *tag*, *metric* and *metric-type* of the set rule of route-map take precedence over the ones configured for the redistribute command.

The metric value of the route-map associated should be in the range of 0 to 16777214. If the metric value is not in this range, the route cannot be introduced.

The rules for the **no** form of the **redistribute** command are as follows:

If some parameters are specified in the no command, restore their default settings; If no parameters are specified in the **no** command, delete the whole command.

For example, if the configuration is made below:

Now modify the configuration with the command `no redistribute isis 112 level-2`

According to the above rules, the command only restores level-2 to default and level-2 is default per se, so after the above no command is executed, the configuration remains as

```
redistribute isis 112 level-2
```

To delete the whole command, use the command below

Configuration Examples

The following example redistributes the direct route and associates route-map test :

```
ipv6 router ospf 1
redistribute connect metric 10 route-map test
```

The associated route-map is configured as follows:

```
route-map test permit 10 match metric 20
set metric 30
```

Related Commands

Platform Description

The effect of the above configuration is to set the metric value which is 20 of the redistributed routes to 30, and that of other routes to 10

Command	Description
default-information originate	Sets the default route to be redistributed.
default-metric	Sets the default metric for the route to be redistributed.
summary-prefix	Sets the converged address range of the external route.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

N/A

3.41. router-id

Use this command to set the router ID (device ID). Use the **no** form of this command to restore the default setting.

router-id *router-id*

no router-id

Parameter Description

Parameter	Description
<i>router-id</i>	ID of the device in the IPv4 address format.

Defaults

The OSPFv3 routing process, the largest IPv4 address of all loopback interfaces is elected as the router ID; If there is no loopback interface with an IPv4 address, the OSPFv3 process will elect the largest IPv4 of all other interfaces as the router ID

Command

Routing process configuration mode

Mode

Usage Guide

Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the format of IPv4 address.

Any IPv4 address can be set as the router ID, but the router ID of every routers in the AS must be unique. If multiple OSPFv3 processes are running on the same device, the router ID of every process must be unique. Note that the change of the router ID results in considerable processing work in the protocol. Therefore, it is not recommended to change any router ID without proper reason. A prompt will be given to ask whether you are sure to modify the router ID. It is recommended that you specify a router ID once an OSPFv3 process starts before configuring other parameters for the process

Configuration Examples

Related Commands

Platform Description

The following example sets the ID of the device that participates in the OSPFv3 process to 1.1.1.1.

```
router-id 1.1.1.1
```

Command	Description
ipv6 ospf priority	Sets the interface priority.
show ipv6 ospf	Displays the OSPFv3 routing process information.

N/A

3.42. summary-prefix

Use this command to configure the converged route outside the OSPFv3 routing domain in the routing process configuration mode. Use the **no** form of this command to restore the default settings. **summary-prefix** *ipv6-prefix/prefix-length* [**not-advertise** | [**tag** *number*] [**cost** *cost*]]

no summary-prefix *ipv6-prefix/prefix-length* [**not-advertise** | [**tag**] [**cost**]]

Parameter Description

Parameter	Description
<i>ipv6-prefix/prefix-length</i>	Address range of the converged route
not-advertise	Does not advertise the converged route to neighbors. Absence of this parameter means to advertise.
tag <i>number</i>	Tag value redistributed to the OSPFv3 inner route, in the range from 0 to 4294967295.
cost <i>cost</i>	Cost value of converged route, in the range from 0 to 16777214.

Defaults

No converged route is configured by default.

Command Mode

Routing process configuration mode.

Usage Guide

When routes are redistributed by another routing process into the OSPFv3 routing process, every route is advertised to the OSPFv3-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous system border device can advertise only one converged route, thus reducing the scale of routing table greatly.

It is different from the **area range** command. The area range involves the convergence of routes between OSPFv3 areas, while the **summary-prefix** involves the convergence of external routes of the OSPFv3 routing domain.

Configuring the **summary-prefix** command on the ASBR can perform convergence for only redistributed routes; while configuring this command on the NSSA ABR translator can

perform convergence for the redistributed routes and the Type-5 routes translated from Type-7.

Configuration Examples

Related Commands

Platform Description

The following example configures the external route within the 2001:DB8::/64 to the converged route 2001:DB8::/64 to advertise it.

```
summary-prefix 2001 :DB8 : :/64
```

Command	Description
area-range	Configures route convergence between the OSPFv3 areas.
redistribute	Redistributes the routes in other routing process.

N/A

3.43. show ipv6 ospf

Use this command to display the information of the OSPFv3 process.

```
show ipv6 ospf [ process-id ]
```

Parameter Description

Parameter	Description
<i>process- id</i>	OSPF process ID number.

Defaults

N/A

Command Mode

Privileged EXEC mode

Configuration Examples

The following example displays the information about the OSPFv3 process.

```
QTECH# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes Enable two-way-maintain
SPF schedule delay 5 secs, Hold time between SPFs 10 secs Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs Maximum wait time for LSA throttle 5000 msecs Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
LSA interval 5 secs, Minimum LSA arrival 1000 msecs Pacing lsa-group: 30 secs
Number of incoming current DD exchange neighbors 0/5 Number of outgoing current DD exchange neighbors 0/5 Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0 Number of LSA originated 11 Number of LSA received 4
Log Neighbor Adjacency Changes : Enabled Number of areas in this router is 2 Area BACKBONE(0)
Number of interfaces in this area is 1(1) SPF algorithm executed 4 times
Number of LSA 3. Checksum Sum 0x1DDF1 Number of Unknown LSA 0

Area 0.0.0.1 (NSSA)
Number of interfaces in this area is 1(1) SPF algorithm executed 5 times
Number of LSA 7. Checksum Sum 0x445FE
Number of Unknown LSA 0
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
default-information originate	Sets the default route to be redistributed.
default-metric	Sets the default metric for the route to be redistributed.
<i>router-id</i>	Sets the OSPFv3 routing process ID

timers spf	Sets the delay and the minimum and maximum intervals for the OSPFv3 to perform SPF calculation after receiving the topology change information.
-------------------	---

Platform Description

N/A

3.44. show ipv6 ospf database

Use this command to display the database information of the OSPFv3 process

show ipv6 ospf [*process-id*] **database** [*lsa-type* [**adv-router** *router-id*]]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID number
<i>lsa-type</i>	The LSA types are as follows: NSSA-external-LSA, AS-external-LSAs, Link-LSAs, Inter-Area-Prefix-LSAs, Inter-Area-Router-LSAs, Intra-Area-Prefix-LSAs, Network-LSAs, Router-LSAs If this parameter is not specified, all LSA information will be displayed.
adv-router <i>router-id</i>	Displays the LSA information generated by the specified router.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following example displays the information about the OSPFv3 process database.

```
QTECH# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface FastEthernet 1/0)
Link State ID      ADV Router    Age Seq#      CkSum Prefix
0.0.0.2            1.1.1.1.      197 0x80000001 0x7cd8
0.0.0.5            2.2.2.2.      206 0x80000001 0x8c86
Link-LSA (Interface Loopback 1)
Link State ID      ADV Router    Age Seq#      CkSum Prefix 0.0.64.1      1.1.1.1
82 0x80000001 0xb760      0
Router-LSA (Area 0.0.0.0)
Link State ID      ADV Router    Age Seq#      CkSum      Link
0.0.0.0            1.1.1.1.      17 0x80000006 0x62a1      1
0.0.0.0            2.2.2.2.      156 0x80000003 0x8653      1
Network-LSA (Area 0.0.0.0)
Link State ID      ADV Router    Age Seq#      CkSum
0.0.0.5            2.2.2.2      157 0x80000001 0xf8f6
Router-LSA (Area 0.0.0.1)
Link State ID      ADV Router    Age Seq#      CkSum      Link
0.0.0.0            1.1.1.1      17 0x80000002      0x0529      0
Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID      ADV Router    Age Seq#      CkSum
```

```
0.0.0.1            1.1.1.1      77 0x80000002 0x83b4
AS-external-LSA
Link State ID      ADV Router    Age Seq#      CkSum
0.0.0.1            1.1.1.1      1 0x80000001 0x6035 E2
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description

N/A

3.45. show ipv6 ospf interface

Use this command to display the OSPFv3 interface information.

show ipv6 ospf [*process- id*] **interface** [*interface-type interface-number* | **brief**]

Parameter Description

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Specifies the interface type and interface number.
<i>process- id</i>	OSPFv3 process ID
brief	Displays the interface summary.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following example displays the information about the OSPFv3 interface.

```
QTECH# show ipv6 ospf interface FastEthernet 1/0 is up, line protocol is up
Interface ID 2
```

IPv6 Prefixes

```
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address) OSPFv3 Process (1), Area
0.0.0.0, Instance ID 0
```

```
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 26 sent 26, DD received
5 sent 4
```

```
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
```

```
LS-Ack received 6 sent 2, Discarded 0
```

Related Commands

Command	Description
---------	-------------

ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.

Platform Description

N/A

3.46. show ipv6 ospf neighbor

Use this command to display the neighbor information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **neighbor** [**interface-type** *interface-number* [**detail**]]
neighbor-id
 [detail | statistics]

Parameter Description

Parameter	Description
<i>process- id</i>	OSPFv3 process ID number
detail	Displays details about the neighbor.
<i>interface-type</i> <i>interface-number</i>	Interface type and interface number
<i>neighbor-id</i>	Neighbor's router ID

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following command displays the brief information about the OSPFv3 neighbor.

```
QTECH# show ipv6 ospf neighbor
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:
```

```
Neighbor ID Pri State Dead Time Interface Instance ID 2.2.2.2 1 Full/DR
00:00:33 FastEthernet 1/0 0
QTECH# show ipv6 ospf neighbor detail
```

```
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c In the area 0.0.0.0 via
interface FastEthernet 1/0 Neighbor priority is 1, State is Full, 6 state changes
DR is 2.2.2.2 BDR is 1.1.1.1 Options is 0x000013 (-|R|-|-|E|V6) Dead timer due in
00:00:36 Database Summary List 0
Link State Request List 0
Link State Retransmission List 0 BFD session state up
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.
area virtual-link	Configures the OSPFv3 virtual link.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description

N/A

3.47. show ipv6 ospf restart

Use this command to display the OSPFv3 graceful restart configuration.

show ipv6 ospf [*process-id*] restart

Parameter Description

Parameter	Description
<i>process-id</i>	OSPFv3 process ID number.

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the restarter status.

```
QTECH# show ipv6 ospf restart Routing Process is ospf 1 Graceful-restart enabled Restart
grace period 120 secs
Current Restart status is plannedRestart
```

```
Current Restart remaining time 50 secs Graceful-restart helper support enabled
```

```
QTECH# show ipv6 ospf restart Routing Process is ospf 1
Neighbor 10.1.1.2, interface addr 10.1.1.2
In the area 0.0.0.0 via interface GigabitEthernet 6/0/0 Graceful-restart helper enabled
Current helper status is helping
Current helper remaining time 50 secs
```

The following example displays the helper status.

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description

N/A

3.48. show ipv6 ospf route

Use this command to display the OSPFv3 route information.

show ipv6 ospf [*process-id*] **route** [**count**]

Parameter Description

Parameter	Description
<i>process- id</i>	OSPFv3 process ID number.
count	Total number of OSPFv3 routes

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide N/A**Configuration Examples**

The following example displays the information about OSPFv3 routes.

```
QTECH# show ipv6 ospf route OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
Destination Metric  Next-hop
E2 2001:DB8:1::/64  1/20   via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O  2001:DB8:2::/64  11     via fe80::c800:eff:fe84:1c, FastEthernet 1/0,
Area 0.0.0.0
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description

N/A

3.49. show ipv6 ospf summary-prefix

Use this command to display the external route convergence information of OSPFv3

show ipv6 ospf [*process- id*] summary-prefix

Parameter Description

Parameter	Description
<i>process- id</i>	OSPFv3 process ID number

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide **N/A****Configuration Examples**

The following example displays the external route convergence information of OSPFv3.

```
QTECH# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:db8::/64,Metric 16777215,Type0,Tag0,Match count0,advertise
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
summary-prefix	Configures the converge route outside the OSPFv3 routing domain.

Platform Description

N/A

3.50. show ipv6 ospf topology

Use this command to display the topology information about each area of OSPFv3.

show ipv6 ospf [*process- id*] topology [*area area-id*]

Parameter Description

Parameter	Description
<i>process- id</i>	OSPFv3 process ID number

<i>area-id</i>	Area ID
----------------	---------

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```
QTECH# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID    Bits Metric  Next-Hop
Interface
1.1.1.1      B  --
2.2.2.2      EB  1  2.2.2.2/fe80::21a:a9ff:fe41:5b06
GigabitEthernet 0/6
OSPFv3 paths to Area (0.0.0.1) routers
Router ID    Bits Metric  Next-Hop
Interface 1.1.1.1 V B  --
2.2.2.2      VEB 1      2.2.2.2/fe80::21a:a9ff:fe41:5b06
GigabitEthernet 0/6
```

The following command displays the topology information about each area of OSPFv3

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
area range	Configures the address range of the OSPF area.

Platform Description

N/A

3.51. show ipv6 ospf virtual-links

Use this command to display the virtual link information of the OSPFv3 process

show ipv6 ospf [*process- id*] virtual-links

Parameter Description

Parameter	Description
<i>process- id</i>	OSPFv3 process ID number

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following command displays the information about the OSPFv3 virtual link.

```
QTECH# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 2.2.2.2 is down
Transit area 0.0.0.1 via interface FastEthernet 1/0, instance ID 0 Local address *
Remote address 3333::1/128
Transmit Delay is 1 sec, State Down,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08 Adjacency state Full
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
area virtual-link	Configures the OSPFv3 virtual link.

show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
--------------------------------	---

Platform Description

N/A

3.52. timers lsa arrival

Use this command to configure a delay for receiving repeated LSAs. Use the **no** form of this command to restore the default setting.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

Parameter	Description
<i>arrival-time</i>	Specifies the delay for receiving repeated LSAs. The range is from 0 to 600000 in the unit of milliseconds.

Defaults

The default is 1000.

Command Mode

Routing process configuration mode

Usage Guide

Configure the device not to process repeated LSAs received within the specific delay.

Configuration Examples

The following example sets the delay for receiving repeated LSAs to 2 seconds.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# timers lsa arrival 2000
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information, including identifiers of routing devices.

Platform Description

N/A

3.53. timers pacing lsa-group

Use this command to set an LSA group pace interval. Use the **no** form of this command to restore the default setting.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter Description

Parameter	Description
seconds	Specifies the LSA group pace interval. The range is from 10 to 1800 in the unit of seconds. The default value is 30.

Defaults

The default is 30.

Command Mode

Routing process configuration mode

Usage Guide

Each LSA has its own lifetime, that is, LSA aging time. An LSA existing for 1800s will be refreshed so that the living time of the LSA will not exceed its aging time. This ensures that normal LSAs are not

cleared due to timeout of aging time. If update and aging operations of each LSA are separately computed, a large number of CPU resources will be consumed.

To effectively utilize CPU resources, configure the device to group LSAs for uniform refreshment. The time for refreshing a group of LSAs is called an LSA group pace interval. Grouping refreshment is to put the LSAs to be refreshed within an LSA group pace interval into a group and refresh them uniformly.

When the number of LSAs is fixed, a longer LSA group pace interval will allow the CPU to process more LSAs when the timer expires for one time. To keep the stability of the CPU, you are recommended not to set an over long LSA group pace interval. This prevents the CPU from processing excessive LSAs when the timer expires each time. If the CPU processes a large number of LSAs each time, it is recommended to shorten the LSA group pace interval. For example, if the database has 10000 LSAs, you need to reduce the LSA

group pace interval. If it has only 40 to 100 LSAs, you can adjust the group pace interval to 10 through 20 minutes.

Configuration Examples

The following example sets the LSA group pace interval to 120 seconds.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)#timers pacing lsa-group 120
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 configuration information.

Platform Description

N/A

3.54. timers pacing lsa-transmit

Use this command to set an interval for sending LSA groups. Use the no form of this command to restore the default setting.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

Parameter	Description
<i>transmit-time</i>	Specifies the interval for sending LSA groups. The range is from 10 to 1000 in the unit of milliseconds.
<i>transmit-count</i>	Specifies the number of LS-UPD packets in an LSA group. The range is from 1 to 200.

Defaults

The default transmit-time is 40 and the transmit-count is 1.

Usage Guide

There are usually a lot of LSAs on a network; therefore, the load of the device is very high. Setting proper **transmit-time** and **transmit-count** values can restrict flooding of LS-UPD packets on the network.

When the CPU load is not high and network bandwidth usage is not large, you can reduce the

transmit-time value and increase the **transmit-count** value to accelerate route convergence.

Configuration Examples

The following example sets the interval for sending LS-UPDs to 50 milliseconds and the specified 20 packets to be sent each time.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information.

Platform Description

N/A

3.55. timers spf

Use this command to set the delay and interval for the OSPFv3 to calculate SPF after receiving the topology change. Use the **no** format of this command to restore the default setting.

timers spf *delay holdtime*

no timers spf

Parameter Description

Parameter	Description
<i>spf-delay</i>	Defines the waiting time for the SPF calculation, which ranges from 0 to 2147483647 seconds. After receiving the topology change information, the OSPF routing process has to wait for a given period before making the SPF calculation.
<i>spf-holdtime</i>	Defines the interval between two SPF calculations, which ranges from 0 to 2147483647 seconds. If the interval has not passed even if the waiting time has elapsed, no SPF calculation can be made yet.

Defaults

There are two default situations: 1. The versions earlier than OS 10.4 do not support the command **timers throttle spf**. The system default is **timers spf 5 10**. 2. The OS 10.4 and

the later versions do support the command **timers throttle spf**, where **timer spf** takes no effect by default.

The delay for SPF calculation is subject to the default setting of the command **timers throttle spf**. Refer to the description of the command.

Usage Guide

The smaller the *spf-delay* and *spf-holdtime*, the shorter time the OSPF takes to adapt to the topology change, but the more CPU time will be used of the router.

The **timer spf** configuration and the **timers throttle spf** configuration will overwrite each other.

Configuration Examples

```
QTECH(config)# ipv6 router ospf 20
QTECH(config-router)# timers spf 3 9
```

The following example sets the delay and holdtime of the OSPFv3 to 3 seconds and 9 seconds respectively.

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the function of the OSPFv3.
show ipv6 ospf	Displays the OSPFv3 routing process information.
timers throttle spf	Configures the exponential backoff delay of the SPF calculation

Platform Description

N/A

3.56. timers throttle lsa all

Use this command to configure an exponential backoff algorithm for generating LSAs. Use the **no**

form of this command to restore the default setting. **timers throttle lsa all delay-time hold-time max-wait-time no timers throttle lsa all**

Parameter Description

Parameter	Description
<i>delay-time</i>	Specifies a shortest LSA generation delay, in milliseconds (the first batch of LSAs is usually generated immediately). The range is from 0 to 600000 in the unit of milliseconds.
<i>hold-time</i>	Specifies a shortest interval between the first two times of LSA refreshment, in milliseconds. The range is from 1 to 600000 in the unit of milliseconds.
<i>max-wait-time</i>	Specifies a longest interval for consecutive two times of LSA refreshment, in milliseconds. The value is used to determine whether LSAs are refreshed consecutively. The range is from 1 to 600000 in the unit of milliseconds.

Defaults

The default *delay-time* is 0, *hold-time* is 5000 and *max-wait-time* is 5000.

Mode**Usage Guide**

If high route convergence capability is needed when links are changed, set a small *delay-time* value.

To reduce CPU consumption, you can properly increase the values of the parameters.

The *hold-time* value cannot be smaller than the *delay-time* value and must be smaller than or equal to the *max-wait-time* value.

Configuration Examples

The following example sets *delay-time* to 10 milliseconds, *hold-time* to one second, and *max-wait-time* to five seconds.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information.

Platform Description

N/A

3.57. timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default setting. **timers throttle route { inter-area *ia-delay* | ase *ase-delay* }**

no timers throttle route { inter-area | ase }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
<i>ia-delay</i>	Sets the delay time of the inter-area route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the <i>ia-delay</i> time runs out.
ase	Calculates the external routes.
<i>ase-delay</i>	Sets the delay time of the external route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the <i>ase-delay</i> time runs out.

Defaults

The default *ia-delay* is 0 and *ase-delay* is 0.

Mode

Usage Guide

The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration Examples

The following example sets the delay time of the inter-area route calculation to one second.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.58. timers throttle spf

Use this command to configure, the delay for SPF calculation as well as the minimum and maximum intervals between two SPF calculations after receiving the topology change information for OSPFv3 in the routing process configuration mode. Use the **no** form of this command to restore the default setting.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
<i>spf-delay</i>	Specifies an SPF calculation delay after the topology change information is received. The range is from 1 to 600000 in the unit of milliseconds.
<i>spf-holdtime</i>	Specifies a shortest interval between two SPF calculations. The range is from 1 to 600000 in the unit of

	milliseconds.
<i>spf-max-waittime</i>	Specifies a longest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.

Defaults

Command Mode

Routing process configuration mode.

Usage Guide

Spf-delay refers to the delay from the topology change to the SPF calculation. *Spf-holdtime* refers to the minimum interval between the first and the second SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval till it reaches to *spf-max-waittime*. If

the interval between two SPF calculations has exceeded the required minimum value, the interval of SPF calculation will re-start from *spf-holdtime*.

Smaller *spf-delay* and *spf-holdtime* value can make the topology convergence faster. Greater

spf-max-waittime value can reduce the SPF calculations. Those configuration are flexible according to the actual stability of the network topology.

Compared with the timers *spf* command, this command is more flexible. It not only speeds up the SPF convergence calculation, but also reduces the system resources consumption of SPF calculation as the topology changes continuously. Therefore, the timers throttle *spf* command is recommended.

- The *spf-holdtime* cannot be smaller than *spf-delay*, or the *spf-holdtime* will be set to be equal to *spf-delay*;
- The *spf-max-waittime* cannot be smaller than *spf-holdtime*, or the *spf-max-waittime* will be set to be equal to *spf-holdtime* automatically;
- The configuration of the timers *spf* command and of the timers throttle *spf* command are overwritten each other.
- With neither timers *spf* command nor timers throttle *spf* command configured, the default value refers to the default of the timers throttle *spf* command

Configuration Examples

The following example configures the delay and holdtime and the maximum time interval of the OSPFv3 as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the time for SPF calculation is: five milliseconds, one second, three seconds, seven seconds, 15 seconds, 31

seconds, 63 seconds, 89 seconds, 179 seconds, 179+90 seconds...

```
QTECH(config)# ipv6 router ospf 20
```

```
QTECH(config-router)# timers spf 5 1000 90000
```

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the OSPFv3 function.
show ipv6 ospf	Displays the routing process information of the OSPFv3
timers spf	Configures the SPF calculation delay .

Platform Description

N/A

3.59. two-way-maintain

Use this command to enable two-way OSPFv3 maintenance. Use the no form of this command to disable this function.

two-way-maintain no two-way-maintain

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Two-way OSPFv3 maintenance is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

Sometimes, there are a lot of sent and received packets on a network, occupying large CPU and memory resources. As a result, some packets cannot be processed immediately or are directly lost. If hello packets from a neighbor cannot be processed within the dead interval of neighbors, the connection with the neighbor will be interrupted due to connection

timeout. If two-way OSPFv3 maintenance is enabled and a large number of packets exist on the network, besides hello packets, the two-way neighboring relationship between the device and the neighbor can also be maintained by DD, LSU, LSR, and LSAck packets from the neighbor. This prevents the neighboring relationship from failing due to receiving delay or discarding of hello packets.

Configuration Examples

The following example disables two-way OSPFv3 maintenance.

```
QTECH(config)# ipv6 router ospf 1
QTECH(config-router)# no two-way-maintain
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.

Platform Description

N/A

4. IS-IS COMMANDS

4.1. address-family ipv6

Use this command to enter the **address-family ipv6** mode. Use the **no** form of this command to delete all configurations in the **address-family ipv6**.

address-family ipv6 [*unicast*]

no address-family ipv6 [*unicast*]

Parameter Description

Parameter	Description
<i>unicast</i>	IPv6 unicast address prefix.

Defaults

By default, no address-family ipv6 is configured.

Command Mode

IS-IS routing process configuration mode

Usage Guide

This command is used for the IPv6 special configurations.

To exit to the IS-IS routing process configuration mode, use the **exit-address-family** command.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# address-family ipv6 unicast
```

Related Commands

Command	Description
exit-address-family	Exits the address-family ipv6 mode.

Platform Description

N/A

4.2. adjacency-check

Use this command to detect protocols supported by the adjacency in the Hello packets. Use the **no**

form of this command is to cancel this detection.

adjacency-check no adjacency-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, this detection is enabled.

Command Mode

IS-IS routing process configuration mode or address-family ipv6 mode

Usage Guide N/A

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# adjacency-check
QTECH(config-router)# address-family ipv6
QTECH(config-router-af)# adjacency-check
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.3. rea-password

Use this command to set the plain-text authentication password for the Level-1 area. Use the **no** form of this command to cancel the password set.

area-password [0 | 7] *password-string* [**send-only**]

no area-password [**send-only**]

Parameter Description

Parameter	Description
0	Indicates that the key is displayed in plaintext.
7	Indicates that the key is displayed in ciphertext.
<i>password-string</i>	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
send-only	Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticate.

Defaults

By default, no authentication password is set.

Command Mode

IS-IS routing process configuration mode

Usage Guide

Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-1 areas and include authentication information in these packets before they are sent. All IS-IS devices in an area must be configured with the same password.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no area-password** command. If you run the **no area-password send-only** command, only the **send-only** setting is canceled. If you run the **area-password psw send-only** and **no area-password send-only** commands in sequence, the configuration is changed to **area-password psw**.

Configuration Examples

The following example specifies the authentication in the IS-IS area using the plaintext mode with the password being *redgiant* and the password applicable to the packets sent only, but not to the packets received.

```
QTECH(config)# router isis
QTECH(config-router)# area-password redgiant send-only
```

Related Commands

Command	Description
domain-password	Sets the Level-2 domain password.
authentication mode	Specifies the IS-IS authentication mode.

Platform Description

N/A

4.4. authentication key-chain

Use this command to specify the key-chain used by the IS-IS authentication.

Use the **no** form of this command to cancel the key-chain specified.

authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>name-of-chain</i>	Key-chain name with the maximum length being 255.
level-1	Specifies the authentication key-chain of the Level-1.
level-2	Specifies the authentication key-chain of the Level-2.

Defaults

By default, the authentication key-chain is not specified.

Command Mode

IS-IS routing process configuration mode

Usage Guide

If the **key chain** command is not used to configure the corresponding key-chain, the authentication will not be performed. In addition, to make the IS-IS key-chain authentication effective, you need to configure the **authentication mode** command at the same time.

This key-chain can apply to the plain-text authentication mode and MD5 encrypted authentication mode. You can use the **authentication mode** command to set the authentication mode.

The length of the password key-string in the key-chain shall not be larger than 80 characters if the plain-text authentication mode is used, otherwise this configuration will fail.

Only one key-chain is used at one time. So, when configuring this command, the said key-chain will be replaced by the new specified one.

If the Level is not specified, the key-chain will apply to both Level-1 and Level-2.

The key-chain specified by this command works on the LSP, CSNP and PSNP packets. The IS-IS will send or receive the password that belongs to this key-chain.

There may contain multiple passwords in the key-chain. When sending the packets, use the password with small number first. While receiving the packets, the packet will be received as long as the password of this packet received corresponds to any password in the key-chain.

```
QTECH(config)# router isis
QTECH(config-router)# authentication key-chain kc level-1
```

Configuration Examples

The following example specifies the authentication in the IS-IS area using the key-chain named *kc*:

Related Commands

Command	Description
authentication mode	Specifies the IS-IS authentication mode.
authentication send-only	Specifies the IS-IS authentication applicable to the sent packets only, but not to packets received.
key-chain	Configures the key-chain.

Platform Description

N/A

4.5. authentication mode

Use this command to specify the mode of IS-IS authentication. Use the **no** form of this command to cancel the specified IS-IS authentication mode.

authentication mode { md5 | text } [level-1 | level-2]

no authentication mode { md5 | text } [level-1 | level-2]

Parameter Description

Parameter	Description
md5	Specifies the MD5 authentication mode to use.
text	Specifies the plain-text authentication mode to use.
level-1	Specifies the authentication mode taking effect on the Level-1.
level-2	Specifies the authentication mode taking effect on the Level-2.

Defaults

By default, the authentication mode is not specified.

Command Mode

IS-IS routing process configuration mode

Usage Guide

To make the key-chain configured by the authentication key-chain command effective, you must use the authentication mode command to specify the authentication mode.

If no Level is specified, the authentication mode specified is applicable to both Level-1 and Level-2. When configuring the **authentication mode** command, if the **area-password** or **domain-password** command has been executed to configure the plaintext authentication before, the said commands will be overwritten by the new command.

If the **authentication mode** command has been configured, the **area-password** or **domain-password** will not be configured successfully, you need to delete the **authentication mode** command first.

Configuration Examples

The following example specifies authentication in the IS-IS area to be the MD5 authentication mode.

```
QTECH(config)# router isis
QTECH(config-router)# authentication mode md5 level-1
```

Related Commands

Command	Description
area-password	Sets the area plaintext authentication password.
authentication key-chain	Specifies the key-chain used by the IS-IS authentication.
authentication send-only	Specifies the IS-IS authentication applicable to the packets sent only, but not to the packets received.
domain-password	Sets the domain plaintext authentication password.

Platform Description

N/A

4.6. authentication send-only

Use this command to specify the IS-IS authentication only applicable to the packets sent, but not to the packets received. Use the **no** form of this command to perform the authentication on the packets received.

authentication send-only [level-1 | level-2]

no authentication send-only [level-1 | level-2]

Parameter Description

Parameter	Description
-----------	-------------

level-1	Specifies setting send-only on the Level-1.
level-2	Specifies setting send-only on the Level-2.

Defaults

By default, this command is not configured. If the IS-IS authentication is configured, the authentication will be performed on the packets both sent and recieved.

Command Mode

IS-IS routing process configuration mode

Usage Guide

With this command configured, the IS-IS will set the authentication password in the packets sent, however, the authentication will not be performed on the packets received. It can apply to the following two occasions: 1. before deploying the IS-IS authentication for all devices in the network. 2. before changing the authentication password or authentication mode. Before the above two tasks start, you need to configure the **authentication send-only** command first to make each device perform no authentication on the packets received, so as to avoid the network oscillation caused during the subsequent authentication password deployment. After the deployment of the entire network authentication finished, execute the **no isis authentication send-only** command to cancel the **send-only** authentication mode.

This command can apply to the plain-text authentication mode and MD5 authentication mode. You can use the **authentication mode** command to set the authentication mode.

If the Level is not specified, the authentication mode specified is applicable to both Level-1 and Level-2.

Configuration Examples

The following example specifies the authentication in the IS-IS area to be the **send-only** mode.

```
QTECH(config)# router isis
QTECH(config-router)# authentication send-only level-1
```

Related Commands

Command	Description
authentication key-chain	Specifies the IS-IS authentication key-chain.
authentication mode	Specifies the mode of IS-IS authentication.
key-chain	Configures the key-chain.

Platform Description

N/A

4.7. bfd all-interfaces

Use this command to configure all interfaces running the IS-IS protocol to conduct BFD link detection.

bfd all-interfaces [anti-congestion]

Use the **no** form of this command to configure all interfaces running the IS-IS protocol to not conduct BFD link detection.

no bfd all-interfaces [anti-congestion]

Parameter Description

Parameter	Description
anti-congestion	IS-IS BFD anti-flapping option

Defaults

The IS-IS support for BFD is disabled on all interfaces by default.

Command Mode

IS-IS routing process configuration mode

Default Level

14

Usage Guide

There are two methods for enabling or disabling the IS-IS support for BFD on interfaces.

Method 1: In IS-IS routing process configuration mode, run the [**no**] **bfd all-interfaces**

[anti-congestion] command to enable or disable the IS-IS support for BFD on all interfaces running the IS-IS protocol.

Method 2: In interface configuration mode, run the **isis bfd [disable | anti-congestion]** command to enable or disable the IS-IS support for BFD on a specified interface.

In normal cases, the BFD function enables to send detection packets to detect the link status at an interval of several milliseconds. When a link exception such as link interruption occurs, the BFD function enables to rapidly detect the link exception, and notify a device running the IS-IS protocol to delete neighbors and delete neighbor availability information from LSP packets. The device running the IS-IS protocol performs route re-calculation and generates a new route, to bypass the failure link, thereby implementing fast convergence. With the introduction of some new technologies such as the

Multi-Service Transport Platform (MSTP), link congestion easily occurs in peak hours. When congestion occurs, the BFD function allows to rapidly detect a link exception, notify a device running the IS-IS protocol to delete a neighbor and delete neighbor availability information from LSP packets, and perform link switching to bypass the congested link. The interval for an IS-IS neighbor to send a Hello detection packet is 10 seconds and the timeout time is 30 seconds. When an exception is detected via the BFD function, IS-IS Hello packets can be normally received, an IS-IS neighbor relationship can be rapidly established, and the route is restored to pass the congested link. Then, BFD is performed again. If there is still a link exception, link switching is performed again, and the process repeats. The route switches between the congested link and other links and flapping occurs.

The anti-flapping function can be enabled to prevent route flapping in the case of link congestion. After the anti-flapping function is enabled, if a link is congested, the IS-IS neighbor status keeps alive but the neighbor availability information in LSP packets is deleted, and the route switches to a non-congested link. After the link is restored, that is, congestion is removed, the neighbor availability information is restored in LSP packets, and the route switches back to the originally congested link, thereby preventing route flapping.

When IS-IS anti-flapping is enabled, the BFD anti-flapping command (**bfd up-dampening**) must be configured on an interface. The two commands must be configured simultaneously. If only one of them is configured, the anti-flapping function does not take effect or a network exception is incurred.

For details about how to enable the BFD anti-flapping function on an interface, see the configuration example of the ISIS BFD command.

Before the IS-IS support for BFD is configured, a BFD session must be configured on an interface. When the BFD anti-flapping command is configured on an interface, if the IS-IS support for BFD is

already configured on the interface, the anti-flapping function must be enabled for a device running the IS-IS protocol.

When the IS-IS anti-flapping option is configured, the BFD anti-flapping command must be configured on an interface.

Configuration Examples

The following example configures all interfaces running the IS-IS protocol to conduct BFD.

```
QTECH(config)# router isis 123
QTECH(config-router)# bfd all-interface
```

4.8. clear clns neighbors

Use this command to clear all IS-IS neighbor relation tables.

clear clns neighbors

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used in the condition of needing to refresh the IS-IS neighbor relation table immediately.

Configuration Examples

Related Commands

Platform Description

The following example clears all IS-IS neighbor relation tables.

```
QTECH# clear clns neighbors
```

Command	Description
clear isis	Clears all IS-IS data structure.

N/A

4.9. clear isis *

Use this command to clear the data structure of all IS-ISs.

clear isis *

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide This command is used in the condition of needing to refresh the LSP immediately. For example, after executing the **area-password** and **domain-password** commands, the previous LSPs still exist in this router, you can use this command to clear these LSPs.

Configuration Examples

Related Commands

Platform Description

QTECH# clear isis *

Command	Description
clear clns neighbors	Clears all IS-IS neighbors.

N/A

4.10. clear isis counter

Use this command to clear various statistics of IS-IS.

clear isis [*tag*] **counter**

Parameter Description

Parameter	Description
<i>tag</i>	IS-IS instance

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

The following example clears various statistics of IS-IS.

QTECH# **clear isis counter**

Command	Description
clear isis *	Clears the data structure of all IS-ISs.

Platform Description

N/A

4.11. default-information originate

Use this command to generate a default routing information and advertise it by LSP. Use the **no** form of this command to delete the default routing information from LSP.

default-information originate [**route-map** *map-name*]

no default-information originate [**route-map** *map-name*]

Parameter Description

Parameter	Description
<i>map-name</i>	(Optional) Associated route-map's name, with the maximum length being 32. By default, the route-map is not associated.

Defaults

By default, there is no default route.

Command Mode

IS-IS routing process configuration mode or address-family ipv6 mode.

Usage Guide

The default route is not generated in the Level-2 domain. Use this command to allow the default route to enter the Level-2 domain.

Configuration Examples

The following example generates a default routing information and advertises it by LSP

```
QTECH(config)# router isis
QTECH(config-router)# default-information originate
QTECH(config-router)# address-family ipv6 QTECH(config-
router-af)# default-information originate
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.12. distance

Use this command to set the management distance of the IS-IS routes. Use the **no** form of this command to restore the default settings.

distance *my-cost*

no distance

Parameter Description

Parameter	Description
<i>my-cost</i>	Distance value in the range of 1 to 255.

Defaults

By default, the distance is 115.

Command Mode

IS-IS routing process configuration mode or IS-IS address-family ipv6 configuration mode

Usage Guide

Use this command to configure the management distance of the IS-IS routes. The shorter the management distance, the more reliable the routing information is.

Configuration Examples

The following example sets the management distance of the IS-IS routes.

```
QTECH(config)# router isis
QTECH(config-router)# distance 100
```

Related Commands

Command	Description
isis metric	Sets the metric value of the interface.

Platform Description

N/A

4.13. domain-password

Use this command to set the plain-text authentication password of Level-2 domain. Use the **no** form of this command to cancel the password configured.

domain-password [0 | 7] *password-string* [**send-only**]
no domain-password [**send-only**]

Parameter Description

Parameter	Description
0	Indicates that the key is displayed in plaintext.
7	Indicates that the key is displayed in ciphertext.
<i>password-string</i>	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
send-only	Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticated.

Defaults

By default, no authentication password is set.

Command Mode

IS-IS routing process configuration mode

Usage Guide

Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-2 domains and include authentication information in these packets before they are sent. All IS-IS devices in a Level-2 domain must be configured with the same password.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no domain-password** command. If you run the **no domain-password send-only** command, only the **send-only** setting is canceled. If you run the **domain-password psw send-only** and **no domain-password send-only** commands in sequence, the configuration is changed to **domain-password psw**.

Configuration Examples

```
QTECH(config)# router isis
```

```
QTECH(config-router)# domain-password redgiant
```

Related Commands

Command	Description
area-password	Sets the plain-text authentication password of Level-1 area.
authentication mode	Specifies the IS-IS authentication mode.

Platform Description

N/A

4.14. enable mib-binding

Use this command to bind MIBs with an IS-IS process. Use the no form of this command to unbind the MIB from the IS-IS process.

enable mib-binding no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, MIBs are bound with IS-IS process 1.

Command Mode

IS-IS routing process configuration mode

Usage Guide

By default, MIBs are bound with IS-IS process 1. The IS-IS process support multiple processes. The administrator can use this command to bind MIBs with the IS-IS process.

Configuration Examples

The following example binds the MIB with an IS-IS process.

```
QTECH# configure terminal
QTECH(config)# router isis
QTECH(config-router)# enable mib-binding
```

Related Commands

Command	Description
graceful-restart helper disable	Disables the IS-IS GR Help capability.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform Description

N/A

4.15. enable traps

Use this command to enable the system to send one or multiple types of IS-IS trap packets. Use the

no form of this command to disable the system to send IS-IS trap packets.

enable traps { all | traps set }

no enable traps { all | traps set }

Parameter Description

Parameter	Description
all	Indicates all types of IS-IS trap packets.
<i>traps set</i>	Indicates the specified type of IS-IS trap packet.

Defaults

By default, no IS-IS trap is sent.

Command Mode

IS-IS routing process configuration mode

Usage Guide There are 18 types of IS-IS packets. The IS-IS packets can be classified into multiple sets. Each set includes several types of trap packets. To enable the system to send the IS-IS trap packet, you need to enable the global IS-IS trap using the **snmp-server enable traps isis** command, specify the host to receive the IS-IS trap packets, and use the **enable traps { all | traps set }** command to specify the type of IS-IS trap packet to be sent.

Configuration Examples

The following example enables the system to send all IS-IS trap packets to the host of IP address 192.168.1.1.

```
QTECH# configure terminal
QTECH(config)#snmp-server enable
traps isis
QTECH(config)#snmp-server host 10.1.1.1 traps version 2c public

QTECH(config)#router isis
QTECH(config-router)# enable traps all
```

Related Commands

Command	Description
graceful-restart helper disable	Disables the IS-IS GR Help capability.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform Descriptio

N/A

4.16. exit-address-family

Use this command to exit IS-IS address family IPv6 configuration mode and return to IS-IS routing process configuration mode.

exit-address-family

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

IS-IS address-family IPv6 configuration mode

Usage Guide

N/A

Configuration Examples

The following example exits IS-IS address family IPv6 configuration mode.

```
QTECH (config-router-af)#exit-address-family
QTECH (config-router)#
```

Related Commands

Command	Description
graceful-restart helper disable	Disables the IS-IS GR Help capability.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform

N/A

4.17. graceful-restart

Use this command to enable the IS-IS GR Restart capability. Use the **no** form of this command to disable this capability.

graceful-restart

no graceful-restart**Parameter Description**

Parameter	Description
N/A	N/A

Defaults

IS-IS GR is enabled by default.

Command Mode

IS-IS routing process configuration mode

Usage Guide

Use this command to enable the IS-IS GR Restart capability. As long as the network conditions remain unchanged, IS-IS can be restarted and restored to the pre-restart state without impact on data forwarding.

Configuration Examples

The following example enables the IS-IS GR Restart capability.

```
QTECH(config)# router isis
QTECH(config-router)# graceful-restart
```

Related Commands

Command	Description
graceful-restart helper disable	Disables the IS-IS GR Help

	capability.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform Description

N/A

4.18. graceful-restart grace-period

Use this command to configure the maximal interval for the graceful-restart. Use the **no** form of this command to restore the default interval.

graceful-restart grace-period **seconds**

no graceful-restart grace-period

Parameter

Parameter	Description
<i>seconds</i>	Time interval allowed for the device graceful-restart, in the range of 1 to 65,535 seconds.

Defaults

The default value is 300 seconds.

Command Mode

IS-IS routing process configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the interval of the grace-restart to 40 seconds.

```
QTECH(config)# router isis
```



```
QTECH(config-router)# graceful-restart grace-period 40
```

Related Commands

Command	Description
graceful-restart	Enables the IS-IS GR Restart capability.
show isis graceful-restart	Displays the status information of the IS-IS GR Restart.

Platform Description

N/A

4.19. graceful-restart helper disable

Use this command to disable the IS-IS GR Helper capability. Use the **no** form of this command to enable this capability.

graceful-restart helper disable

no graceful-restart helper disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

IS-IS GR Helper capacity is enabled by default.

Command Mode

IS-IS routing process configuration mode

Usage Guide

To disable the IS-IS GR Helper capability, execute this command. In this case, the IS-IS will ignore the request of graceful-restarting the device.

Configuration Examples

The following example disables the IS-IS GR Helper capability.

```
QTECH(config)# router isis
```

Related Commands

Platform Description

```
QTECH(config-router)# graceful-restart helperdisable
```

Command	Description
graceful-restart	Enables the IS-IS GR Restart capability.

N/A

4.20. hello padding

Use this command to pad IS-IS Hello packets.

```
hello padding [ multi-point | point-to-point ]
```

Use the **no** form of this command to cancel the padding of IS-IS Hello packets.

```
no hello padding [ multi-point | point-to-point ]
```

Parameter Description

Parameter	Description
multi-point	Pads Hello packets of the LAN type.
point-to-point	Pads Hello packets of the P2P type.

Defaults

Padding is enabled for Hello packets of the LAN type and P2P type by default.

Command Mode

IS-IS routing process configuration mode

Default Level

14

Usage Guide

Hello packets can be padded to notify a neighbor of the MTU supported by the local device. You can use this command to set whether to pad all Hello packets sent by the IS-IS process. You can also separately specify the type of Hello packets for padding, for example, you can set not to pad all Hello packets of the LAN type or not to pad all Hello packets of the P2P type.

The **isis hello padding** command is available in interface configuration mode. Hello packets sent by a specific interface are not padded if the padding of such Hello packets is cancelled in IS-IS routing process configuration mode or the padding of Hello packets sent by the interface is cancelled in interface configuration mode.

Configuration Examples

The following example configures to cancel the padding of Hello packets of the P2P type.

```
QTECH(config)# router isis
QTECH(config-router)# no hello padding point-to-point
```

4.21. hostname dynamic

Use this command to replace the System ID of the router with the destination router's hostname. Use the **no** form of this command to cancel this replacement.

hostname dynamic

no hostname dynamic

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the hostname dynamic function is disabled.

Command Mode

IS-IS routing process configuration mode

Usage Guide With this command configured, the hostname of the destination router replaces the System ID. The System IDs shown in the execution of the command such as **show isis database**, **show isis neighbors** are all replaced by the hostname of the destination router.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# hostname dynamic
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.22. ignore-lsp-errors

Use this command to ignore the LSP checksum errors. Use the **no** form of this command to not ignore the LSP checksum errors.

ignore-lsp-errors

no ignore-lsp-errors

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the LSP checksum errors are not ignored.

Command Mode

IS-IS routing process configuration mode

Usage Guide

When the local IS-IS receives a LSP, it will calculate the checksum of LSP received and compare the calculated checksum with that in the LSP packets. By default, if the checksum in the LSP packets is different from the checksum calculated, this LSP will be discarded without processing. If we execute the ignore-lsp-errors command to ignore the checksum errors, the LSP packets with the incorrect checksum will be processed as the normal packets.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# ignore-lsp-errors
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.23. ip router isis

Use this command to enable the IPv4 IS-IS on the specified interface. Use the no form of this command to disable the IPv4 IS-IS routing on the specified interface.

ip router isis [tag]

no ip router isis [tag]

Parameter Description

Parameter	Description
tag	IS-IS instance name.

Defaults

By default, the Ipv4 IS-IS is disabled on the interface.

Command Mode

Interface configuration mode

Usage Guide

Use this command to enable the IS-IS IPv4 routing protocol on the interface. The no form of this command disables the IS-IS IPv4 routing.

If the no ipv4 unicast-routing is executed in global configuration mode, the IS-IS will disable the IPv4 routing function on all interfaces, namely execute the no ipv4 router isis [tag] on all interfaces automatically, while other IS-IS configurations will remain unchanged.

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
```

```
QTECH(config-if)# ip router isis
```

Related Commands

Command	Description
ipv6 router isis	Enables the IPv6 IS-IS on the interface.
router isis	Creates IS-IS instances.

Platform Description

N/A

4.24. ipv6 router isis

Use this command to enable the IPv6 IS-IS routing on the specified interface. This command must be configured in the IS-IS configuration. The interface will run on the IS-IS instance named with Tag. If this IS-IS instance is inexistent or this IS-IS instance is not enabled and not initialized, the interface will not enable the IS-IS routing.

Use the **no** form of this command to disable the IPv6 IS-IS routing on the specified interface.

ipv6 router isis [tag]

no ipv6 router isis [tag]

Parameter Description

Parameter	Description
<i>tag</i>	IS-IS instance name

Defaults

By default, the Ipv6 IS-IS routing is not supported on the interface.

Command Mode

Interface configuration mode

Usage Guide Configure this command to enable the IS-IS IPv6 routing protocol on the interface. The **no** form of this command disables the IS-IS IPv6 routing.

If the **no ipv6 unicast-routing** is executed in the global configuration mode, the IS-IS will disable the IPv6 routing function on all interfaces, namely execute the **no ipv6 router isis**

[*tag*] on all interfaces automatically, while other IS-IS configurations will remain unchanged.

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
```

```
QTECH(config-if)# ipv6 router isis
```

Related Commands

Command	Description
ip router isis	Enables the IPv4 IS-IS on the interface.
router isis	Creates IS-IS instances.

Platform Description

N/A

4.25. isis authentication key-chain

Use this command to set the key-chain used by the IS-IS interface authentication. Use the **no** form of this command to cancel the specified key-chain.

isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>name-of-chain</i>	Key-chain name with the maximum length being 255.
level-1	Specifies the authentication key-chain of the Level-1.
level-2	Specifies the authentication key-chain of the Level-2.

Defaults

By default, no IS-IS interface authentication key-chain is specified.

Command Mode

Interface configuration mode

Usage Guide

If the **key chain** command is not used to configure the corresponding key-chain, the authentication will not be performed. In addition, to make the IS-IS key-chain authentication effective, you need to configure the **isis authentication mode** command at the same time.

This key-chain can apply to the plain-text authentication mode and MD5 encrypted authentication mode. You can use the **isis authentication mode** command to set the authentication mode.

The length of the password key-string in the key-chain shall not be larger than 254 characters if the plain-text authentication mode is used, otherwise this configuration will fail.

Only one key-chain is used at one time. So, when configuring this command, the said key-chain will be overwritten by the new specified one.

If the Level is not specified, the key-chain will apply to both Level-1 and Level-2.

The key-chain specified by this command works on the Hello packets. The IS-IS will send or receive the password that belongs to this key-chain.

There may contain multiple passwords in the key-chain. When sending the packets, use the password with small number first. While receiving the packets, the packet will be received as long as the password of this packet received corresponds to any password in the key-chain.

The authentication commands configured in the IS-IS configuration mode such as authentication key-chain are effective to the LSP, SNP packets, but take no effect on the IS-IS interface.

Configuration Examples

The following example specifies the authentication key-chain of the interface GigabitEthernet 0/1

named as *kc*.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis authentication key-chain kc
```

Related Commands

Command	Description
isis authentication mode	Specifies the mode of IS-IS interface
	authentication.

isis authentication send-only	Specifies the IS-IS interface authentication only applicable to the packets sent, but not to the packets received.
key-chain	Configures the key-chain.

Platform Description

N/A

4.26. isis authentication mode

Use this command to specify the mode of IS-IS interface authentication. Use the **no** form of this command to remove the configuration.

isis authentication mode { md5 | text } [level-1 | level-2]

no isis authentication mode { md5 | text } [level-1 | level-2]

Parameter Description

Parameter	Description
md5	Specifies the MD5 authentication mode.
text	Specifies the plain-text authentication mode.
level-1	Specifies the interface authentication mode to take effect on the Level-1.
level-2	Specifies the interface authentication mode to take effect on the Level-2.

Defaults

By default, no interface authentication mode is specified.

Command Mode

Interface configuration mode

Usage Guide

To make the key-chain configured by the **isis authentication key-chain** command take effect, you must use the **isis authentication mode** command to specify the authentication mode.

If the Level is not specified, the authentication mode specified will apply on both Level-1 and Level-2. When configuring the **isis authentication mode** command, if the isis password has been executed, the set command will be overwritten by this command.

If the **isis authentication mode** command has been executed, the **isis password** will not be configured successfully. So, you need to delete the **isis authentication mode** command first.

Configuration Examples

The following example specifies the authentication mode on the Level-2 of the interface GigabitEthernet 0/1 to be the MD5 authentication mode.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis authentication mode md5 level-2
```

Related Commands

Command	Description
isis authentication key-chain	Specifies the key-chain used by the IS-IS interface authentication.
isis authentication send-only	Specifies the IS-IS interface authentication to only apply on the packets sent, but not on the packets received.
key-chain	Configures the key-chain.
isis password	Sets the plain-text authentication password for the packets transmit on the IS-IS interface.

Platform Description

N/A

4.27. isis authentication send-only

Use this command to specify the IS-IS interface authentication to only apply to the packets sent and not to the packets received. Use the no form of this command to restore the authentication of packets received on the interface.

isis authentication send-only [level-1 | level-2]

no isis authentication send-only [level-1 | level-2]

Parameter Description

Parameter	Description
level-1	Set the send-only on the Level-1 of the interface.
level-2	Set the send-only on the Level-2 of the interface.

Defaults

By default, this command is not configured. If the IS-IS interface authentication has been configured, then the authentication will be performed on the packets sent and received at the same time.

Command Mode

Interface configuration mode

Usage Guide With this command configured, the IS-IS will set the authentication password in the Hello packets sent from the interface, however, the authentication will not be performed on the Hello packets received. It can apply to the following two occasions: 1. before deploying the IS-IS interface authentication for all devices in the network. 2. before changing the authentication password or authentication mode. Before the above two tasks start, you need to configure the isis authentication send-only command first to make each device perform no authentication on the Hello packets received, so as to avoid the network oscillation caused during the subsequent IS-IS interface authentication deployment. After the deployment of the entire network authentication finished, execute the no isis authentication send-only command to cancel the send-only authentication mode.

This command can apply to the plain-text authentication mode and MD5 authentication mode. You

can use the **isis authentication mode** command to set the mode used by the IS-IS interface authentication.

If the Level is not specified, the authentication mode specified is applicable to the Level-1 and Level-2.

Configuration Examples

The following example specifies the authentication on the Level-1 of the interface GigabitEthernet 0/1 using send-only authentication mode.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis authentication send-only level-1
```

Related Commands

Command	Description
isis authentication key-chain	Specifies the key-chain used by the IS-IS interface authentication.
isis authentication mode	Specifies the mode of the IS-IS interface authentication.
key-chain	Configures the key-chain.

Platform Description

N/A

4.28. isis bfd

Use this command to enable association between IS-IS and BFD on an interface.

isis bfd [disable | anti-congestion]

Use the **no** form of this command to disable association between IS-IS and BFD on an interface.

no isis bfd [disable | anti-congestion]

Parameter Description

Parameter	Description
disable	Disables association between IS-IS and BFD on an interface.
anti-congestion	Indicates the IS-IS BFD anti-flapping option.

Defaults

If the **bfd all-interfaces** command is configured, association between IS-IS and BFD is enabled on an interface.

If the **bfd all-interfaces** command is not configured, association between IS-IS and BFD is disabled on an interface.

By default, the anti-flapping function is disabled.

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

There are two methods for enabling or disabling association between IS-IS and BFD on interfaces.

Method 1: In IS-IS routing process configuration mode, run the [**no**] **bfd all-interfaces [anti-congestion]** command to enable or disable association between IS-IS and BFD on all interfaces running the IS-IS protocol.

Method 2: In interface configuration mode, run the **isis bfd [disable | anti-congestion]** command to enable or disable association between IS-IS and BFD on a specified interface.

In normal cases, the device with the BFD function enabled sends detection packets to detect the link status at an interval of several milliseconds. When a link exception such as link interruption occurs, the device with the BFD function enabled rapidly detects the link exception and informs a device running the IS-IS protocol to delete neighbors and delete neighbor availability information from LSP packets. The device running the IS-IS protocol performs route re-calculation and generates a new route, to bypass the failed link, thereby implementing fast convergence. With the introduction of some new technologies such as the Multi-Service Transport Platform (MSTP), link congestion easily occurs in peak hours. When congestion occurs, the device with the BFD function enabled rapidly detects a link exception, informs a device running the IS-IS protocol to delete a neighbor and delete neighbor availability information from LSP packets, and performs link switching to bypass the congested link. The interval for an IS-IS neighbor to send a Hello detection packet is 10 seconds, and the timeout time is 30 seconds. When an exception is detected via the BFD function, IS-IS Hello packets can be normally received, the IS-IS neighbor relationship can be rapidly reestablished, and the route is restored to pass the congested link. Then, BFD is performed again. If there is still a link exception, link switching is performed repeatedly. The route switches between the congested link and other links and flapping occurs.

The anti-flapping function can be enabled to prevent route flapping in the case of link congestion. After the anti-flapping function is enabled, if a link is congested, the IS-IS neighbor keeps alive but the neighbor availability information in LSP packets is deleted, and the route switches to a

non-congested link. After the link is restored, that is, congestion is eliminated, the neighbor availability information is restored in LSP packets, and the route switches back to the originally congested link, thereby preventing route flapping.

When IS-IS anti-flapping is enabled, the BFD anti-flapping command (**bfd up-dampening**) must be configured on an interface. The two commands must be configured simultaneously. If only one of them is configured, the anti-flapping function does not take effect or a network exception is incurred.

Before association between IS-IS and BFD is configured, a BFD session must be configured on an interface.

When the BFD anti-flapping command is configured on an interface, if association between IS-IS and BFD is already configured on the interface, the anti-flapping function must be enabled for a device running the IS-IS protocol.

When the IS-IS anti-flapping option is configured, the BFD anti-flapping command must be configured on an interface.

Configuration Examples

The following example disables association between IS-IS and BFD on GigabitEthernet 0/1.

QTECH(config)# interface GigabitEthernet 0/1

```
QTECH(config-if)# no switchport
QTECH(config-if)# isis bfd disable
```

The following example enables the IS-IS BFD anti-flapping option and configures the BFD anti-flapping command on GigabitEthernet 0/1.

```
QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if)#
no switchport QTECH(config-if)# isis bfd anti-congestion
QTECH(config-if)# bfd up-dampening 60000
```

4.29. isis circuit-type

Use this command to set the circuit-type for the IS-IS interface. Use the **no** form of this command to restore the default settings.

isis circuit-type { level-1 | level-1-2 | level-2-only }

no isis circuit-type

Parameter Description

Parameter	Description
level-1	Forms the Level-1 adjacency.

leve-2-only	Forms the Level-2 adjacency.
level-1-2	Forms the Level-1-2 adjacency.
external	Uses the interface as an external domain interface.

Defaults

By default, the circuit-type is Level-1-2.

Command Mode

Interface configuration mode

Usage Guide If the circuit type is set to Level-1 or Level-2-only, IS-IS will only send PDUs of the corresponding Level.

If the system type is set to Level-1 or Level-2-only, IS-IS only processes the instances of the corresponding Level, and the interface only sends the PDUs of the same Level specified by the **is-type** and **circuit-type** commands.

If the interface is set to **external**, the interface will work as an external domain interface and IS-IS will not send PDUs of the corresponding Level.

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis circuit-type level-2-only
```

Related Commands

Command	Description
isis-type	Sets the Level of IS-IS instance.

Platform Description

N/A

4.30. isis csnp-interval

Use this command to set the interval for broadcasting the CSNP packets on the IS-IS interface, with the unit being second. Use the no form of this command to restore the default interval.

isis csnp-interval *interval* [level-1 | level-2]

no isis csnp-interval [*interval*] [level-1 | level-2]

Parameter Description

Parameter	Description
<i>interval</i>	Interval for sending the CSNP packets in the range of 0 to 65535, with the unit being second.
level-1	Interval for sending the CSNP packets configured only on the Level-1.
level-2	Interval for sending the CSNP packets configured only on the Level-2.

Defaults

By default, in the broadcast network, the interval for sending the CSNP packets is 10 seconds. While in the P2P interface network, no CSNP packet is sent by default.

When using this command without the parameter Level-1 and Level-2, the new setting is defaulted to be applicable to the Level-1 and Level-2 at the time.

Command Mode

Interface configuration mode

Usage Guide

Configure this command to change the interval for sending the CSNP packets. By default, the DIS on the broadcast network sends the CSNP packets every 10 seconds.

For the P2P interface network, by default, the CSNP packets will only be sent at the beginning of adjacency formation. If the interface is set to mesh-groups, you can configure the periodic sending of the CSNP packets.

If the csnp-interval is set to 0, no CSNP packets will be sent.

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis csnp-interval 20
```

Related Commands

Command	Description
---------	-------------

N/A

N/A

Platform Description

N/A

4.31. isis hello-interval

Use this command to set the interval for sending Hello packets on the interface, with the unit being second. Use the **no** form of this command to restore the default interval.

isis hello-interval { *interval* | **minimal** } [**level-1** | **level-2**]

no isis hello-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>interval</i>	Interval for sending the Hello packet, in the range of 1 to 65536.
minimal	The holdtime is set to the minimal value 1.
level-1	This interval applies on the Level-1.
level-2	This interval applies on the Level-2.

Defaults

By default, the interval value is 10 seconds, which is applicable to the Level-1 and Level-2 at the same time.

When using this command without the parameter Level-1 and Level-2, the new setting is defaulted to be applicable to the Level-1 and Level-2 at the time.

Command Mode

Interface configuration mode

Usage Guide

Configure this command to change the interval for sending Hello packets. By default, the multiplier of the Hello holdtime is 3, and the DIS in broadcast network sends Hello packets at an interval which is three times of non-DIS. If this IS is elected as DIS on this interface, the interface will send Hello packets every 3.3 seconds by default.

If the key word "minimal" is used, then the "holdtime" in Hello packets will be set to 1, and hello interval will be calculated based on the hello-multiplier. For example, if hello-multiplier is configured to 4 and "isis hello-interval minimal" is configured at the same time, the value of hello-interval shall be 1s/4 (250ms).

By default, the CPU protection is enabled on the switch, so that the number of packets corresponding to the destination group addresses of ISIS (AllISSystems, AllL1ISSystems, AllL2ISSystems) is limited when they are sent to the CPU, for example, the default limited value is 400pps. The number of packets received by the switch may be larger than the default value if there are many neighbors or the interval for sending Hello packets is short, resulting in continual vibration of the adjacent relation. In this case, you need to raise the

limit of IS-IS packets using the global commands **cpu-protect type isis-is pps**, **cpu-protect type isis-l1is pps** and **cpu-protect type isis-l2is pps**.

Configuration Examples

The following example sets the interval for sending Hello packets on the interface.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis hello-interval 5 level-1
```

The following example sets the Holdtime for sending Hello packets on the interface to the minimum value 1.

```
QTECH(config)# interface GigabitEthernet 0/1
```

Related Commands

Platform Description

QTECH(config-if)# isis hello-interval minimal

Command	Description
isis hello-multiplier	Sets the multiplier of the Hello hold timer.

N/A

4.32. isis hello-multiplier

Use this command to set the multiplier of Hello hold timer. Use the **no** form of this command to restore the default settings.

isis hello-multiplier *multiplier-number* [**level-1** | **level-2**]

no isis hello-multiplier [*multiplier-number*] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>multiplier-number</i>	Multiplier value in the range of 2 to 100.

Defaults

By default, the multiplier is 3..

Command Mode

Interface configuration mode

Usage Guide

Use this command to set the multiplier of Hello holdtime. The holdtime value in the Hello packet is the product of hello-interval and this multiplier.

Configuration Examples

```
uijie(config)# router isis
QTECH(config-router)# isis hello-multiplier 5
```

Related Commands

Command	Description
isis hello-interval	Sets the interval for sending the Hello packets.

Platform Description

N/A

4.33. isis hello padding

Use this command to specify the filling mode for the IS-IS Hello packets. Use the no form of this command to fill no IS-IS Hello packets.

isis hello padding

Parameter Description

Command Mode

no isis hello padding

Parameter	Description
N/A	N/A

Interface configuration mode

Usage Guide Fill the IS-IS Hello packets to advertise the MTU supported to the neighbors. Hello packets can be padded to notify a neighbor of the MTU supported by the local device.

In IS-IS routing process configuration mode, the corresponding hello padding command also exists. Hello packets sent by a specific interface are not padded if the padding of such Hello packets is cancelled in IS-IS routing process configuration mode or the padding of Hello packets sent by the local interface is cancelled in interface configuration mode.

Configuration Examples

The following example fills no IS-IS Hello packets.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# no isis hello padding
```

Related Commands

Command	Description
isis hello-interval	Sets the interval for sending the Hello packets.

Platform Description

N/A

4.34. isis lsp-interval

Use this command to set the interval for the LSP PDU transmission. Use the **no** form of this command to restore the default interval.

isis lsp-interval *milliseconds* [**level-1** | **level-2**] **no isis lsp-interval** [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>milliseconds</i>	Indicates the LSP interval. The value range is 1 to 4,294,967,295, in the unit of milliseconds.
level-1	Applies the setting only to Level-1 LSPs.
level-2	Applies the setting only to Level-2 LSPs.

Defaults

By default, the lsp-interval is 33ms.

Command Mode

Interface configuration mode

Usage Guide **N/A****Configuration Examples**

The following example sets the interval for the LSP PDU transmission to 100.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis lsp-interval 100
```

Related Commands

Command	Description
isis retransmit-interval	Sets the LSP retransmission interval in the P2P network.

Platform Description

N/A

4.35. isis mesh-group

Use this command to add the interface to the specified mesh-group. Use the **no** form of this command to separate the interface from the mesh-group.

isis mesh-group { **blocked** | *mesh-group-id* }

no isis mesh-group

Parameter Description

Parameter	Description
blocked	Blocks all LSP forwarding on the interface.
<i>mesh-group-id</i>	Adds the interface to the mesh-group of specified mesh-group-id with the range being 1 to 4,294,967,295.

Defaults

By default, the interface is not added to any mesh-group.

Command Mode

Interface configuration mode

Usage Guide

Mesh-groups can control the exceeding and redundant LSP spreading in the NBMA network. In the normal condition, the IS-IS router spreads out the LSP from all interfaces except for the receiving one, that is, if a router is configured multiple subinterfaces, the LSP will be sent from all subinterfaces and the neighbors will receive many same LSPs, which wastes a large number of CPU and bandwidth.

The IS-IS mesh-group allows grouping the router interfaces, so if a LSP is received by one subinterface in the group, this LSP will not be spread out through other subinterfaces in the group. And if the router receives the LSP from the interface out of the group, it will spread out the LSP from other interfaces as usual.

If you need to configure the **mesh-group** on the IS-IS interface, use the **isis csnp-interval** command to configure the interval for sending the non-0 CSNP packets, so as to send the CSNP packets regularly to synchronize the LSP and ensure the integrity of LSP synchronization between neighbors in network.

Configuration Examples

```
QTECH#configure terminal
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)#isis mesh-group 1
```

Related Commands

Command	Description
isis network point-to-point	Sets the Broadcast interface type of IS-IS to Point-to-Point.

Platform Description

N/A

4.36. isis metric

Use this command to set the metric for the interface. Use the **no** form of this command to restore the default metric.

isis metric *metric* [**level-1** | **level-2**]

no isis metric [*metric*] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>metric</i>	Metric value in the range of 1 to 63.
level-1	Sets this metric to apply on the Level-1 circuit.
level-2	Sets this metric to apply on the Level-2 circuit.

Defaults

By default, the metric is 10, which applies on both Level-1 and Level-2 circuit.

Command Mode

Interface configuration mode

Usage Guide

The Metric value is in the TLV of the IP reachable information and is applied to the SPF calculation. The greater metric value means the more routing cost on this interface and the longer path calculated by SPF.

This value is effective only when the metric-style includes narrow.

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)#isis metric 1
```

Related Commands

Command	Description
metic-style	Sets the metric type.
isis wide-metric	Sets the wide metric of the IS-IS interface.

Platform Description

N/A

4.37. isis network point-to-point

Use this command to set the IS-IS Broadcast interface to the Point-to-Point type. Use the **no** form of this command to restore the interface type to the Broadcast.

isis network point-to-point no isis network point-to-point

Parameter Description

Parameter	Description
point-to-point	Point-to-Point type interface.

Defaults

By default, it is Broadcast type.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis network point-to-point
```

Related Commands

Command	Description
isis mesh-group	Adds the IS-IS interface into the specified mesh group.

Platform Description

N/A

4.38. isis password

Use this command to set the plain-text authentication password for the Hello packet transmitted on the interface. Use the no form of this command to remove the configurations.

isis password *password-string* [send-only] [level-1 | level-2]

no isis password [send-only] [level-1 | level-2]

Parameter Description

Parameter	Description
0	Indicates that the key is displayed in plaintext.
7	Indicates that the key is displayed in ciphertext.
password-string	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
send-only	Indicates that the plaintext authentication password is only used to authenticate sent packets. Received packets are not authenticated.
level-1	Applies the setting to the Level-1 circuit type.
level-2	Applies the setting to the Level-2 circuit type.

Defaults

By default, both the passwords on the Level-1 and Level-2 are not configured.

Command Mode

Interface configuration mode

Usage Guide

This command is used to set the plain-text authentication password for the Hello packets transmitted on the interface. Use the no form of this command to clear the passwords. When the Level is not specified, the authentication password configured is by default applicable to every Level. If the isis authentication mode command has been executed, this command will not be configured successfully. To configure this command, you need to delete the isis authentication mode command first.

Running the no isis password send-only command can only disable the send-only option.

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis password redgiant
```

Related Commands

Command	Description
isis authentication mode	Specifies the mode of the IS-IS interface authentication.

Platform Description

N/A

4.39. isis priority

Use this command to set the priority for the DIS election on the LAN. Use the no form of this command to restore the default priority.

isis priority *value* [level-1 | level-2]

no isis priority [*value*] [level-1 | level-2]

Parameter Description

Parameter	Description
<i>value</i>	Value of the priority in the range of 0 to 127.
level-1	Applies to the Level-1 circuit.
level-2	Applies to the Level-2 circuit.

Defaults

The default priority value is 64 and it is applied on both Level-1 and Leve-2 circuit.

Command Mode

Interface configuration mode

Usage Guide Use this command to change the priority value in the Hello of LAN.

The low priority value has the lower priority in the DIS election than the high priority value. This command takes no effect on the Point-to-Point network interface.

The no isis priority command is used to restore the priority to the default value no matter whether the parameter is followed. If you want to modify the configured priority, you can either use the isis priority command with parameter specified to overwrite the configured command directly, or configure a new parameter after restoring the priority to the default value.

Configuration Examples

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis priority 127 level-1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.40. isis psnp-interval

Use this command to set the minimum transmission interval of PSNP packets.

isis psnp-interval *seconds* [**level-1** | **level-2**]

Use the **no** form of this command to cancel the specified minimum transmission interval of PSNP packets.

no isis psnp-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description
seconds	Indicates that the value range is 1 to 120 in seconds.

level-1	Indicates that the configuration takes effect only at Level-1.
level-2	Indicates that the configuration takes effect only at Level-2.

Defaults

This command is not configured by default. The default minimum transmission interval is 2 seconds and takes effect both at Level-1 and Level-2.

Command Mode

Interface configuration mode

Default Level **14**

Usage Guide

PSNP packets are used to request for LSP packets or respond to received LSP packets in a point-to-point network. In both cases, it is recommended to send PSNP packets rapidly. If there are excessive LSP packets but the device performance is poor, you can set the PSNP packet transmission interval and LSP retransmission time to larger values, to reduce the device load.

Configuration Examples

The following example sets the PSNP packet transmission interval to 5 seconds for Interface GigabitEthernet 0/1 at Level-2.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)# isis psnp-interval 5 level-2
```

4.41. isis retransmit-interval

Use this command to set the LSP retransmission interval. Use the **no** form of this command to restore the default interval.

isis retransmit-interval *seconds* [**level-1** | **level-2**]

no isis retransmit-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description
-----------	-------------

<i>seconds</i>	Indicates the LSP retransmission interval. The value range is 0 to 65,535, in the unit of seconds.
level-1	Applies the setting only to Level-1 LSPs.
level-2	Applies the setting only to Level-2 LSPs.

Defaults

The default value is 5s.

Command Mode

Interface configuration mode

Usage Guide

Use this command to configure the LSP retransmission interval. In a P2P network, after a device sends an LSP, if the device receives no PSNP response within the time specified by this command, it will resend the LSP. If the retransmission interval is set to 0, the LSP will not be resent.

The following example sets the LSP retransmission interval to 10s.

Configuration Examples

```
QTECH(config)# interface serial 0/1
QTECH(config-if)# isis retransmit-interval 10 level-2
```

Related Commands

Command	Description
isis lsp-interval	Configures the interval for LSP advertisement on the interface.

Platform Description

N/A

4.42. isis subvlan

Use this command to enable IS-IS on super VLANs. Use the **no** form of this command to restore the default setting.

isis subvlan [all | **vid**] no isis subvlan

Parameter Description

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults

The default setting takes effect only on super VLANs with IS-IS disabled.

Command Mode

Interface configuration mode.

Usage Guide

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when IS-IS multicast packets are sent over a super VLAN containing multiple sub VLANs, the IS-IS multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the IS-IS function does not need to be enabled on a super VLAN. Therefore, the IS-IS function is disabled by default. However, in some scenarios, the IS-IS function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration Examples

The following example sends the IS-IS multicast packets to sub VLAN 1024 of super VLAN 300.

```
QTECH(config)# interface vlan 300
QTECH(config-if-VLAN 300)# isis subvlan 1024
```

4.43. isis three-way-handshake disable

Use this command to disable three-way handshake for point-to-point network. Use the **no** form of this command to enable three-way handshake for point-to-point network.

isis three-way-handshake disable

no isis three-way-handshake disable**Parameter Description**

Parameter	Description
N/A	N/A

Defaults

By default, three-way handshake is enabled.

Command Mode

Interface configuration mode

Usage Guide

In the point-to-point network, three-way handshake is enabled by default. That is to say, the IS-IS neighbor can be established only after three-way handshake is successful. You can use this command to cancel three-way handshake negotiation to accelerate IS-IS neighbor establishment or for the the device not supporting three-way handshake.

Configuration Examples

The following example disables three-way handshake on interface GigabitEthernet 0/0.

```
QTECH(config)#int GigabitEthernet 0/0 QTECH(config-if)#  
isis network point-to-point  
QTECH(config-if)# isis three-way-handshake disable
```

Related Commands

Command	Description
metric-type	Sets the metric type.
isis metric	Sets the metric value of the interface.

Platform Description

N/A

4.44. isis wide-metric

Use this command to set the wide metric of the interface. Use the **no** form of this command to restore the default wide metric.

isis wide-metric *metric* [**level-1** | **level-2**]

no isis wide-metric [*metric*] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>metric</i>	Metric value in the range of 1 to 16,777,241.
level-1	Sets this Metric to apply on the Level-1 circuit.
level-2	Sets this Metric to apply on the Level-2 circuit.

Defaults

By default, the metric value is 10 and it is applicable to both Level-1, Level-2 circuit.

Command Mode

Interface configuration mode

Usage Guide

The Metric value is in the TLV of the IP reachable information and is applied to the SPF calculation. The greater metric value means the more routing cost on this interface and the longer path calculated by SPF.

This value is effective only when the metric-style includes wide.

Configuration Examples

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if)#isis wide-metric 1000
```

Related Commands

Command	Description
metric-type	Sets the metric type.
isis metric	Sets the metric value of the interface.

Platform Description

4.45. is-type

Use this command to specify the level for the IS-IS process. Use the no form of this command to restore the default level for IS-IS process.

```
is-type { level-1 | level-1-2 | level-2-only }  
no is-type
```

Parameter Description

Parameter	Description
level-1	Specifies the IS-IS process running on the Level-1 only.
level-1-2	Specifies the IS-IS process running on both Level-1 and Level-2.
level-2-only	Specifies the IS-IS process running on the Level-2 only.

Defaults

By default, the IS-IS process runs on Level-1-2.

Command Mode

IS-IS routing process configuration mode

Usage Guide

Changing the is-type enables or disables the route of one Level.

Configuration Examples

```
QTECH(config)# router isis  
QTECH(config-router)# is-type level-1
```

Related Commands

Command	Description
isis circuit-type	Sets the type of Interface circuit.

Platform Description

N/A

4.46. log-adjacency-changes

Use this command to log the changes of the IS adjacency status in case of debug disabled. Use the

no form of this command to disable this function.

log- adjacency-changes no log- adjacency-changes

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, this function is enabled.

Command Mode

IS-IS routing process configuration mode

Usage Guide

You can also use the **debug** command to log the changes of the IS adjacency status. But using the IS-IS debug command will exhaust large numbers of resources.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# log-adjacency-changes
```

Related Commands

Command	Description
N/A	N/A

4.47. lsp-fragments-extend

Use this command to enable the LSP fragment extension mode for a level. Use the **no** form of this command to disable the LSP fragment extension mode for a level.

```
lsp-fragments-extend [ level-1 | level-2 ] [compatible rfc3786] no lsp-fragments-extend [ level-1 | level-2 ] [compatible rfc3786]
```

Parameter Description

Parameter	Description
level-1	Enables the LSP fragment extension mode for the Level-1 only.
level-2	Enables the LSP fragment extension mode for the Level-2 only.
compatible	Compatible with RFC3786
rfc3786	The older version of extended LSP implementation.

Defaults

By default, LSP fragment extension is disabled.

If no level is specified, the LSP fragment extension mode is enabled for both Level-1 and Level-2.

Command Mode

IS-IS routing process configuration mode

Usage Guide

The originating LSP can be divided up to 256 fragments. After the 256 fragments are filled, the subsequent link state information, such as the neighbor and IP routing, will be discarded, resulting in network problem.

To avoid the above problem, you can enable the LSP fragment extension function, and configure the additional system ID using the **virtual-system** command.

If there are other vendor's device supporting RFC3786 standard in the network, you need to display the link state database of the device when enabling or disabling the **compatible** option. If there is indeed the vendor's device, you can use the **clear isis *** command to clear the remaining LSP packets to trigger the system to update the link state database.

Configuration Examples

The following example enables the LSP fragment extension mode for the Level-2.

```
QTECH(config)# router isis
QTECH(config-router)# lsp-fragments-extend level-2
```

Related Commands

Command	Description
N/A	N/A

4.48. lsp-gen-interval

Use this command to set the minimal interval of the LSP generation. Use the **no** form of this command to restore the default value.

lsp-gen-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval* *hold-interval*]

no lsp-gen-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description
level-1	Applies the configuration only to Level-1.
level-2	Applies the configuration only to Level-2.
<i>maximum-interval</i>	Indicates the maximum interval for generating two consecutive LSP packets. The value range is 1 to 65535 (in seconds). The default value is 5 .
<i>initial-interval</i>	Indicates the waiting time for generating an LSP packet for the first time. The value range is 0 to 60000 (in milliseconds). The default value is 50 .
<i>hold-interval</i>	Indicates the minimum interval for generating an LSP packet for the second time. The value range is 10 to 60000 (in milliseconds). The default value is 200 .

Defaults

By default, this command is not configured and the interval of the minimal generation is 5s, it is effective on both Level-1 and Level-2

Command Mode

IS-IS routing process configuration mode

Usage Guide

The LSP packet generation interval refers to the interval for generating two different LSP packets. A smaller generation interval indicates faster network convergence, which, however, will be accompanied by frequent flooding on the network.

The waiting time for generating an LSP packet for the first time is the initial interval. If the network becomes unstable, the LSP packet regeneration interval is changed to be less than the maximum interval, and the interval for generating an LSP packet for the second time becomes the hold interval. A corresponding penalty will be added to this interval: The next interval for regenerating a LSP packet doubles the previous interval for generating the same LSP packet, until the regeneration interval reaches the maximum interval. Subsequent LSP packets will be generated at the maximum interval. When the network becomes stable, the LSP packet regeneration interval becomes greater than the maximum interval, and the waiting time for LSP packet generation is restored to the initial interval.

Link changes have high requirements for convergence. The initial interval can be set to a small value. The preceding parameters can also be adjusted to larger values to reduce CPU consumption.

The value of **initial-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of **initial-interval** will be used as the value of **maximum-interval**.

The value of **hold-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of

hold-interval will be used as the value of **maximum-interval**.

The value of **initial-interval** cannot be greater than that of **hold-interval**. Otherwise, the value of

initial-interval will be used as the value of **hold-interval**.

Configuration Examples

The following example sets the minimum interval for generating two duplicate LSP packets to 10 seconds, the interval for generating a duplicate LSP packet for the first time to 100 ms, and the interval for generating a duplicate LSP packet for the second time to 200 ms.

```
QTECH(config)# router isis
QTECH(config-router)# lsp-gen-interval 10 100 200
```

The following example sets the minimum interval for generating two duplicate LSP packets to 5 seconds.

```
QTECH(config)# router isis
QTECH(config-router)# lsp-gen-interval 5
```

Related Commands

Command	Description
---------	-------------

isp-refresh-interval	Configures the interval for LSP refresh.
-----------------------------	--

Platform Description

N/A

4.49. isp-length originate

Use this command to set the maximum length for transmitting LSP packets.

isp-length originate *size* [level-1 | level-2]

Use the no form of this command to restore the default value.

no isp-length originate [level-1 | level-2]

Parameter Description

Parameter	Description
<i>size</i>	Specifies the maximum length for transmitting LSP packets. The value range is 512 to 16000 in bytes.
level-1	Indicates that the configuration takes effect only at Level-1.
level-2	Indicates that the configuration takes effect only at Level-2.

Defaults

The default value of the maximum length for transmitting LSP packets is 1492. If no level is specified, the default value is level-1-2, that is, the configuration takes effect at both Level-1 and Level-2.

Command Mode

IS-IS routing process configuration mode

Default Level **14**

Usage Guide In principle, the length of LSP and SNP packets cannot be greater than the interface MTU. Otherwise, LSP packets and SNP packets are directly discarded upon being sent.

Configuration Examples

The following example sets the maximum length for transmitting LSP packets at Level-2 to 1498 bytes.

```
QTECH(config)# router isis 1
QTECH(config-router)# lsp-length originate 1498 level-2
```

4.50. lsp-length receive

Use this command to set the maximum length for receiving LSP packets.

`lsp-length receive` **size**

Use the **no** form of this command to restore the default value.

`no lsp-length receive`

Parameter Description

Parameter	Description
<i>size</i>	Specifies the maximum length of LSP packets. The value range is 1,492 to 16,000 in bytes according to the RFC.

Defaults

The default value is **1492**.

Command Mode

IS-IS routing process configuration mode

Default Level

14

Usage Guide

This command is used to control the maximum length of LSP packets that can be received by the local device. In fact, to prevent a route convergence failure, intermediate nodes need to receive LSP packets with the maximum length of the interface MTU as long as the memory permits. In this sense, this command seems nominal. The maximum length for

receiving LSP packets cannot be less than the maximum length for transmitting LSP packets. If the maximum length for receiving LSP packets is less than the maximum length for transmitting LSP packets, the maximum length for receiving LSP packets is automatically adjusted to the maximum length for transmitting LSP packets.

Configuration Examples

The following example configures the maximum length for receiving LSP packets to 1498 bytes.

```
QTECH(config)# router isis
QTECH(config-router)# lsp-length receive 1498
```

4.51. lsp-refresh-interval

Use this command to set the LSP refresh interval. Use the no form of this command to restore the

Parameter Description

default value.

`lsp-refresh-interval` *interval*

`no lsp-refresh-interval`

Defaults

By default, the `lsp-refresh-interval` is 900 seconds.

Parameter	Description
<i>interval</i>	LSP refresh interval in the range of 1 to 65535 with unit being second.

Command Mode

IS-IS routing process configuration mode

Usage Guidelf the LSP stable status lasts for the time of refresh interval, LSP will refresh this LSP and update the LSP version and publish it.

It should be noted that the `lsp-refresh-interval` must be less than the max lifetime.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# lsp-refresh-interval 600
```


Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.52. max-area-addresses

Use this command to set the maximal number of area address allowed. Use the no form of this command to restore the default value.

`max-area-addresses value`

`no max-area-addresses`

Parameter Description

Parameter	Description
<i>value</i>	The maximal number of area address allowed, in the range of 3 to 6.

Defaults

By default, the max-area-addresses is 3.

Command Mode

IS-IS routing process configuration mode

Usage Guide

For the IS routers of Level-1, only the ones with the same max-area-addresses are allowed to establish the adjacency relation.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# max-area-addresses 5
```

Related Commands

Command	Description
net	Sets the IS-IS NET(Network Entry Title) address.

Platform Description

N/A

4.53. maximum-paths

Use this command to set the maximum number of IS-IS equal-cost routing entries in the routing table.

maximum-paths *maximum*

Use the **no** form of this command to restore the default value.

no maximum-paths

Parameter Description

Parameter	Description
<i>maximum</i>	Maximum number of IS-IS equal-cost routing entries in the routing table. The value range is 1 to device capacity .

Defaults

The default value is **2**.

Command Mode

IS-IS routing process configuration mode, IS-IS address-family IPv6 configuration mode

Default Level **14**

Usage Guide

This command is used by the IS-IS protocol to control the number of IS-IS equal-cost routing entries in the routing table. The routing table itself also has a command for controlling the number of equal-cost routing entries. The effective number of equal-cost routing entries is the smaller of the two values.

Configuration Examples

The following example sets the maximum number of IS-IS IPv4 equal-cost routing entries in the routing table to **5**.

```
QTECH(config)# router isis
QTECH(config-router)# maximum-paths 5
```

The following example sets the maximum number of IS-IS IPv6 equal-cost routing entries in the routing table to **6**.

```
QTECH(config)# router isis
QTECH(config-router)# address-family ipv6
QTECH(config-router-af)# maximum-paths 6
```

4.54. max-lsp-lifetime

Use this command to set the maximum value of the LSP lifetime. Use the **no** form of this command to restore the default value.

max-lsp-lifetime *value*

no max-lsp-lifetime

Parameter Description

Parameter	Description
<i>value</i>	Maximum value of the LSP lifetime in the range of 1 to 65,535, with unit being second.

Defaults

By default, the max-lsp-lifetime is 1200 seconds.

Command Mode

IS-IS routing process configuration mode

Usage Guide

It should be noted that the max-lsp-lifetime must be greater the lsp-refresh-interval 300.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# max-lsp-lifetime 1500
```

Related Commands

Command	Description
lsp-refresh-interval	Configures the interval for LSP refresh.

Platform Description

N/A

metric-style

Use this command to set the metric style. Use the no form of this command to restore the default metric style.

```
metric-style { narrow [ transition ] | wide [ transition ] | transition } [ level-1 | level-1-2 | level-2 ]
```

```
no metric-style { narrow [ transition ] | wide [ transition ] | transition } [ level-1 | level-1-2 | level-2 ]
```

```
| ]
```

Parameter Description

Parameter	Description
narrow	Uses the old metric style with the router interface metric ranging from 1 to 63.
wide	Uses the new metric style with the router interface metric ranging from 1 to 16777214
transition	Allows the router to send and receive the new and old metric style.
level-1	This metric-style on the Level-1 circuit.
level-2	This metric-style applies on the Level-2 circuit.
level-1-2	This metric-style applies on the Level-1-2 circuit.

Defaults By default, the metric-style is narrow.

Command Mode

IS-IS routing process configuration mode

Usage Guide

The metric value of the interface is specified by the **isis metric** *metric* when the metric-style is set to narrow, while the metric value is specified by the **isis wide-metric** *metric* in case that the metric-style is set to wide or **transition**.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# metric-style wide
```

Related Commands

Command	Description
isis metric	Sets the metric of the interface.
isis wide-metric	Sets the wide metric of the interface.

Platform Description

N/A

4.55. multi-topology

Use this command to enable IS-IS to support IPv6 unicast topology. Use the **no** form of this command to restore the default setting.

multi-topology [transition]

no multi-topology [transition]

Parameter Description

Parameter	Description
transition	Configures the MT transition mode.

Defaults

By default, multitopology is not configured, namely, IS-IS does not support IPv6 unicast topology.

Command Mode

IS-IS address-family IPv6 configuration mode

Usage Guide 1.

When this command is not configured, IPv4 and IPv6 share the same IS-IS physical topology, which is also called default topology.

If the **transition** parameter is not specified, the device runs in multi-topology mode, the IS-IS v4 process works in the default topology while the IS-IS v6 process works in the IPv6 unicast topology.

If the **transition** parameter is specified, the device runs in multi-topology transition mode and the IS-IS v6 process runs in both the default topology and IPv6 unicast topology.

The above three configurations are exclusive.

The device which runs in multi-topology transition mode can transmit the multi-topology TLV and the default topology TLV. The multi-topology transition mode can be applied in incremental deployment to ensure smooth network migration. However, this mode may cause leaking of routes between the default topology and IPv6 unicast topology. Be careful to configure multi-topology transition mode, as this configuration may lead to network problems such as route blackhole and network loop.

Before you configure this command, you need to set the metric style as wide or transition mode. Configuring the metric style as narrow and configuring only one Level to support wide or transition mode will disable the multitopology routing (MTR) function.

Configuration Examples

The following example configures multi-topology.

```
QTECH(config)# router isis
QTECH(config-router)# address-family ipv6 QTECH(config-router-af)# multi-topology
```

Related Commands

Command	Description
router isis	Creates IS-IS instances.

Platform Description

N/A

4.56. net

Parameter Description

Use this command to set the IS-IS NET (Network Entry Title) address. Use the no form of this command to delete this NET address.

net net-address

no net net-address

Parameter	Description
<i>net-address</i>	The format of net-address is shown as below: XX..XXXX.YYYY.YYYY.YYYY.00, the XX...XXXX is the area address and the YYYY.YYYY.YYYY is the system ID.

Defaults

By default, no NET address is set.

Command Mode

IS-IS routing process configuration mode

Usage Guide This command is used to set the Area ID and System ID for the IS-IS.

Up to three NET addresses are allowed to be set by default, namely three addresses with different Area can be set. However, the System ID must be the same.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# net 49.0000.0001.0002.0003.00
```

Related Commands

Command	Description
router isis	Creates IS-IS instances.

Platform Description

N/A

4.57. passive-interface

Use this command to configure the passive interface. Use the **no** form of this command to remove the passive interface.

passive-interface [**default**] { *interface-type* *interface-number* }

no passive-interface [**default**] { *interface-type* *interface-number* }

Parameter Description

Parameter	Description
default	Configures IS-IS disabled interfaces as passive.
<i>interface-type</i>	Indicates the interface type.
<i>interface-number</i>	Indicates the interface number.

Defaults

The passive interface is not configured by default.

Command Mode

IS-IS routing process configuration mode

Usage Guide Use this command to disable the interface to receive and send the IS-IS packets, but to advertise the IP address of the interface.

After the **default** option is configured, if the number of IS-IS disabled interfaces exceeds 255, the first 255 interfaces are configured as passive and the remaining interfaces are non-passive.

Configuration Examples

The following example configures interface GigabitEthernet 0/0 as passive.

```
QTECH(config)# router isis 1
```

Related Commands

Platform Description

```
QTECH(config-router)# passive-interface GigabitEthernet0/0
```

Command	Description
---------	-------------

router isis	Creates IS-IS instances.
--------------------	--------------------------

N/A

4.58. redistribute

Use this command to redistribute the routes from one routing protocol into another routing protocol. Use the **no** form of this command to delete the redistribution.

redistribute { **bgp** | **ospf** *process-id* **match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] } }

rip | **connected** | **static** } [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*] [**level-1** | **level-1-2** | **level-2**]

no redistribute { **bgp** | **ospf** *process-id* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** |

2] }] | **rip** | **connected** | **static** } [**metric** *metric-value*] [**metric-type** { **internal** | **external** }] [**route-map** *map-tag*] [**level-1** | **level-1-2** | **level-2**]

Parameter Description

Parameter	Description
process-id	OSPF process ID, in the range of 1 to 65535.
match { internal external [1 2] nssa-external [1 2] }	Redistributes the OSPF routes to perform the filtering on the subtype of the OSPF routes. If the match option is not specified, all routes of the ospf subtype by default are received. If the 1 or 2 followed by the match external is not specified, then redistribute the route of the OSPF external1 and external 2. if the 1 or 2 following the match nssa-external is not specified, then redistribute the routes of OSPF nssa-external 1 and nssa-external 2.
metric metric-value	Sets the metric value of redistributing the route, in the range of 0 to 4261412864. If the metric option is not specified, the external metric value is used.

metric-type { internal external }	Sets the metric type of redistributing the route. internal: use the internal metric type. external: use the external metric type. If the metric-type is not specified, the internal type is used by default.
route-map map-tag	Sets the route-map during the external routes redistribution, which is used to filter the redistributed routes or set attributions of the routes. The name of map-tag shall not be over 32 characters. No route-map is configured by default.
level-1 level-1-2 level-2	Specifies the Level of receiving the redistributed routing information. If the Level is not specified, it is defaulted to be redistributed into the Level-2 .
	The format is shown as below: level-1: redistribute into the Level-1 level-1-2: redistribute into both Level-1 and Level-2. level-2: redistribute into the Level-2.

Defaults By default, no redistribution is configured.

Command Mode

IS-IS routing process configuration mode , IS-IS address-family ipv6 mode

Usage Guide

Configure "**no redistribue { bgp | ospf processs-id | rip | connected | static }**" to disable protocol redistribution. If "**no redistribute**" is followed by any other parameter, it means that this parameter is restored to the default setting instead of disabling protocol redistribution. For example: "**no redistribute bgp**" will disable bgp redistribution, while "**no redistribute bgp route-map aa**" will disable route-map aa filtering during redistribution instead of disabling bgp redistribution.

The routing information will be placed into the IP External Reachability Information TLV of LSP when redistributing external route in the IPv4 mode.

The routing information will be placed to the IPv6 Reachable TLV of LSP when redistributing external route in the IPv6 mode.

In the old version of some vendors, after configuring the **metric-type** to the **external**, the redistributed route metric will be added by 64 and then perform the routing according to the metric value during the routing calculation, which violates the protocol. In actual application,

the priority of the external route may be higher than that of the internal route. When connecting with these old version of some vendors, the related configuration (such as the **metric** or the **metric-type**) of each device can be modified to ensure that the priority of the internal route is higher than the external.

Configuration Examples

Related Commands

Platform Description

The following example sets the metric value to 10.

```
QTECH(config)# router isis
QTECH(config-router)# redistribute ospf 1 metric 10 level-1
```

Command	Description
redistribute isis [tag] level-2 into level-1	Redistributes the reachable routing information from Level-2 into Level-1.
redistribute isis [tag] level-1 into level-2	Redistributes the reachable routing information from Level-1 into Level-2.
route-map	Configures the route map.

N/A

4.59. redistribute isis level-1 into level-2

Use this command to redistribute the Level-1 reachable routing information of the IS-IS instance into

Parameter Description

the Level-2 of current instance. Use the **no** form of this command to disable this redistribution. **redistribute isis [tag] level-1 into level-2 [route-map route-map-name | distribute-list access-list-name]**

no redistribute isis [tag] level-1 into level-2 [route-map route-map-name | distribute-list

Parameter	Description
<i>tag</i>	Name of the IS-IS instance.
route-map <i>map-name</i> <i>route-</i>	<p>Sets the route map during the route redistribution, which is used to filter the redistributed route and set attributions of this route.</p> <p>Name of the <i>route-map-name</i> shall not be over 32 characters.</p> <p>No route-map is configured by default.</p>
distribute-list <i>access-list-name</i>	<p>Uses the distribute-list to filter the redistributed routes.</p> <p>Access-list-name is the prefix list associated, it can be the standard, extended or naming prefix list. The format is shown as below:</p> <p>{<1-99> <100-199> <1300-1999> <2000-2699> <i>acl-name</i>}</p> <p>In the IS-IS address-family ipv6 mode, you can use only the naming prefix list with the format being <i>acl-name</i>.</p>

Defaults

If the IS-IS Level-2 instance exists, all IS-IS Level-1 routes are by default redistributed into the IS-IS Level-2 instance.

Command Mode

IS-IS routing process configuration mode or IS-IS **address-family ipv6** mode.

Usage Guide

Use the **route-map** or **distribute-list** to filter the Level-1 route of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into the Level-1 of current instance.

You can only choose one of the two parameters **route-map** and **distribute-list**.

Configure the **no distribute isis [tag] level-2 into level-1** to disable the specified instance redistribution. If the **no redistribute** is followed by any other parameters, it means that this parameter is restored to the default setting instead of disabling the specified instance redistribution.

For example: "**no redistribute isis tag1 level-1 into level-2**" will disable the isis tag1 redistribution, while " **no redistribue isis tag1 level-1 into level-2 route-map aa** " will disable route-map aa filtering during redistribution instead of disabling the isis tag1 redistribution.

Configuration Examples

```
QTECH(config)# router isis aa
QTECH(config-router)# redistribute isis bb level-1 into level-2
```

Related Commands

Command	Description
redistribute	Redistributes the routing information from
	another routing protocol.
redistribute isis level-2 into level-1	Redistributes the reachable routing information from Level-2 into Level-1.

Platform Description

N/A

4.60. redistribute isis level-2 into level-1

Use this command to redistribute the Level-2 reachable routing information of the IS-IS instance into the Level-1 of current instance. Use the **no** form of this command to remove the redistribution. **redistribute isis** [*tag*] **level-2 into level-1** [**route-map** *route-map-name* / **distribute-list**

access-list-name / **prefix** *ip-address net-mask*]

no redistribute isis [*tag*] **level-2 into level-1** [**route-map** *route-map-name* / **distribute-list**

access-list-name / **prefix** *ip-address net-mask*]

Parameter Description

Parameter	Description
-----------	-------------

<i>tag</i>	Name of the IS-IS instance to be redistributed.
route-map <i>route-map-name</i>	<p>Sets the route map during the route redistribution, which is used to filter the redistributed routes and set attributions of the routes.</p> <p>Name of the <i>route-map-name</i> shall not be over 32 characters.</p> <p><input type="checkbox"/> No route-map is configured by default.</p>
distribute-list <i>access-list-name</i>	<ul style="list-style-type: none"> • Uses the distribute-list to filter the redistributed routes. • Access-list-name is the prefix list associated, it can be the standard, extended or naming prefix list. The format is shown as below: <ul style="list-style-type: none"> <input type="checkbox"/> {<1-99> <100-199> <1300-1999> <2000-2699> <i>acl-name</i>} • In the IS-IS address-family ipv6 mode, you can use only the naming prefix list with the format being <i>acl-name</i>.

Defaults

N/A

Command Mode

IS-IS routing process configuration mode or IS-IS **address-family ipv6** mode.

Usage Guide

Use the **route-map** or **distribute-list** to filter the Level-2 route of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into the Level-1 of current instance.

You can only choose one of the two parameters **route-map** and **distribute-list**.

Configure the **no redistribute isis [tag] level-2 into level-1** to disable the specified instance redistribution. If the **no redistribute** is followed by any other parameters, it means that this parameter is restored to the default setting instead of disabling the specified instance redistribution.

For example: "**no redistribute isis tag1 level-2 into level-1**" will disable the isis *tag1* redistribution, while "**no redistribute isis tag1 level-2 into level-1 route-map a**" will disable route-map aa filtering during redistribution instead of disabling the isis *tag1* redistribution.

Configuration Examples

```
QTECH(config)# router isis aa
```

```
QTECH(config-router)# redistribute isis bb level-2 into level-1
```

Related Commands

Command	Description
redistribute	Redistributes the routing information from another routing protocol.
redistribute isis level-1 into level-2	Redistributes the reachable routing information from Level-1 into Level-2.

Platform Description

N/A

4.61. router isis

Use this command to create the IS-IS instance. Use the **no** form of this command to delete this instance.

router isis [*tag*]

no router isis [*tag*]

Parameter Description

Parameter	Description
<i>tag</i>	Instance name

Defaults

By default, no IS-IS instance is configured.

Command Mode

Global configuration mode

Usage Guide

Use this command to initialize the IS-IS instance and enter the IS-IS routing process configuration mode.

The IS-IS instance will not be executed unless one NET address is configured at least.

When enabling the IS-IS routing process with the parameter *tag*, the parameter *tag* will be used as well when disabling the IS-IS routing process.

By default, the CPU protection is enabled on the switch, so that the number of packets corresponding to the destination group addresses of ISIS (AllISSystems, AllL1ISSystems, AllL2ISSystems) is limited when they are sent to the CPU, for example, the default limited value is 400pps. The number of packets received by the switch may be larger than the default value if there are many neighbors or the interval for sending Hello packets is short, resulting in continual vibration of the adjacent relation. In this case, you need to raise the limit of IS-IS packets using the global commands **cpu-protect type**

isis-is pps, cpu-protect type isis-l1is pps **and** cpu-protect type isis-l2is pps.

```
QTECH# configure terminal
QTECH(config)# router isis
```

Configuration Examples

Related Commands

Command	Description
ip router isis	Enables the IS-IS IPv4 routing protocol on the interface.
ipv6 router isis	Enables the IS-IS IPv6 routing protocol on the interface.
net	Sets the NET address.

Platform Description

N/A

4.62. set-overload-bit

Use this command to instruct a neighbor not to use the local IS-IS node as a transit device for forwarding data.

set-overload-bit [**on-startup** *seconds*] [**suppress** { [**interlevel**] [**external**] }] [**level-1** | **level-2**]

Use the **no** form of this command to disable the function of instructing a neighbor not to use the local IS-IS node as a transit device for forwarding data.

no set-overload-bit [level-1 | level-2]

Parameter Description

Parameter	Description
on-startup seconds	Indicates that an IS-IS node automatically enters the OVERLOAD state after restart. seconds is the duration of the IS-IS node in the OVERLOAD state after restart. The value range is 5 to 86,400 in seconds.
suppress	Indicates that internal routes (IS-IS inter-area routes and intra-area routes) or external routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state.
interlevel	Indicates that IS-IS inter-area routes and intra-area routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state. It is used in combination with the suppress keyword.
external	Indicates that external routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state. It is used in combination with the suppress keyword.
level-1	Sends LSP packets that carry the OVERLOAD bit only to Level-1 neighbors.
level-2	Sends LSP packets that carry the OVERLOAD bit only to Level-2 neighbors.

Defaults

The function of instructing a neighbor not to use the local IS-IS node as a transit device for forwarding data is disabled by default.

Command Mode

IS-IS routing process configuration mode

Default Level

14

Usage Guide

This command forces a IS-IS node to set the OVERLOAD bit in non-virtual LSP packets, to instruct IS-IS neighbors not to use the local node as a transit device.

If the **on-startup** keyword is carried, the device automatically enters the OVERLOAD state after restart. If the **on-startup** keyword is not carried, the device immediately enters the OVERLOAD state upon restart.

The **on-startup** keyword takes effect for only one level.

The OVERLOAD bit is mainly used in the following cases:

Device overload

The overload of the local IS-IS node, for example, memory insufficiency or CPU full load, may cause incomplete routes in the local routing table or no resource for data forwarding. You can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local node as a transit device.

In this case, the **on-startup** keyword is not carried in the configuration. The OVERLOAD bit is manually set or cancelled. You must manually cancel this command after the local IS-IS node restores to the normal state. Otherwise, the local IS-IS node is always in the OVERLOAD state

Instantaneous black hole

In the scenario described in RFC3277, the IS-IS converges faster than BGP does. After an IS-IS node restarts, the route fails instantaneously, that is, instantaneous black hole occurs. You can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local node as a transit device till the specified timer expires.

In this case, the configuration must carry the **on-startup** field. The OVERLOAD bit is automatically set or cancelled by the IS-IS node based on the configuration.

After the **on-startup** field is selected, the IS-IS node automatically enters the instantaneous black hole state after restart. After a new neighbor relationship is established, the IS-IS node immediately sends the LSP packet that carries the OVERLOAD bit to notify the neighbor that the local device enters the instantaneous black hole state (or OVERLOAD state) and that the local node cannot be used as a transit device.

When the specified timer expires, the IS-IS node immediately sends the LSP packet without the OVERLOAD bit to notify the neighbor that the local device is no longer in the instantaneous state (or OVERLOAD state) and can be used as a transit device.

The timer time needs to be set based on the number of routes in the network. If there are many routes, set it to a large value; if there are a few routes, set it to a small value.

The local IS-IS node is not intended to be used for forwarding real data

If the local IS-IS node needs to be connected to the production network for testing or other function requirements and it is not intended to be used for forwarding real data in the network, you can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local device as a transit device.

In this case, the **on-startup** field is not carried in the configuration and the OVERLOAD bit is manually set or cancelled.

You can configure **suppress** as required to restrict the routing information carried in LSP packets in the OVERLOAD state, for example, suppress internal routes and external routes and advertise only local direct routes.

Configuration Examples

The following example sets an IS-IS node to immediately enter the instantaneous black hole state after restart till the specified timer expires (set the specified waiting time to 300 seconds) and advertises only local direct routes to neighbors.

```
QTECH(config)# router isis
QTECH(config-router)#set-overload-bit on-startup 300 suppress interlevel external
```

The following example connects the local IS-IS node to the production network as a test device and set its not to forward real data of the production network, to avoid impact on production.

```
QTECH(config)# router isis
QTECH(config-router)#set-overload-bit on-startup 300 suppress interlevel external
```

4.63. spf-interval

Use this command to set the minimal interval for the SPF calculation. Use the **no** form of this command to restore the default minimal interval.

spf-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval* *hold-interval*]

no spf-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description
level-1	Applies the configuration only to Level-1.
level-2	Applies the configuration only to Level-2.
<i>maximum-interval</i>	Indicates the maximum interval for performing two consecutive SPF calculations. The value range is 1 to 120 (in

	seconds). The default value is 10 .
<i>initial-interval</i>	Indicates the waiting time for performing the SPF calculation for the first time. The value range is 0 to 60000 (in milliseconds). The default value is 50 .
<i>hold-interval</i>	Indicates the minimum interval for performing the SPF calculation for the second time. The value range is 10 to 60000 (in milliseconds). The default value is 200 .

Defaults

By default, this command is not configured.

The default SPF interval is 10 seconds, which takes effect at both Level-1 and Level-2.

Command Mode

S-IS routing process configuration mode

Usage Guide

Increasing the maximum interval for performing SPF calculations can avoid frequent SPF calculations and waste of CPU resources. However, a larger minimum interval also leads to slower responses to route changes.

The waiting time for performing the SPF calculation for the first time is the initial interval. If the network becomes unstable, the SPF calculation interval is less than the maximum interval, and the interval for performing the SPF calculation for the second time becomes the hold interval. A corresponding penalty is added to this interval: The next interval for the SPF calculation doubles the previous interval for the same SPF calculation, until the SPF calculation interval reaches the maximum interval. Subsequent SPF calculations are performed at the maximum interval. When the network becomes stable, the interval for performing the SPF calculation becomes greater than the maximum interval, and the waiting time for performing the SPF calculation is restored to the initial interval.

Link changes have high requirements for convergence. The initial interval can be set to a small value. The preceding parameters can also be adjusted to larger values to reduce CPU consumption.

The value of **initial-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of **initial-interval** will be used as the value of **maximum-interval**.

The value of **hold-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of

hold-interval will be used as the value of **maximum-interval**.

The value of **initial-interval** cannot be greater than that of **hold-interval**. Otherwise, the value of

initial-interval will be used as the value of **hold-interval**.

Configuration Examples

The following example sets the maximum interval for generating two duplicate SPF packets to 5 seconds, the interval for generating a duplicate SPF packet for the first time to 100 ms, and the interval for generating a duplicate SPF packet for the second time to 200 ms.

```
QTECH(config)# router isis
QTECH(config-router)# spf-interval 5 100 200
```

The following example sets the maximum interval for generating two duplicate SPF packets to 10 seconds.

```
QTECH(config)# router isis
QTECH(config-router)# spf-interval 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.64. summary-address

Use this command to configure the IPv4 aggregation route. Use the **no** form of this command to delete the aggregation route.

summary-address *ip-address net-mask* [**level-1** | **level-2** | **level-1-2**] [*metric number*]

no summary-address *ip-address net-mask*

Parameter Description

Parameter	Description
<i>ip-address</i>	Indicates the IP address of the summary route.
<i>net-mask</i>	Indicates the subnet mask of the summary route.
level-1	Applies the setting only to Level-1.
level-2	Applies the setting only to Level-2. By default, the setting takes effect

	for Level-2.
level-1-2	Applies the setting to Level-1 and Level-2.
<i>number</i>	Indicates the metric of the summary route.

Defaults

By default, no aggregation route is configured.

Command Mode

IS-IS routing process configuration mode

Usage Guide

With the aggregation route configured, if there is any reachable address or reachable network segment route in the aggregation route, it will publish the aggregation route instead of the detailed route.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# summary-address 10.10.0.0/24 level-1-2
```

Related Commands

Command	Description
summary-prefix	Configures the IPv6 aggregation route.

Platform Description

N/A

4.65. summary-prefix

Use this command to configure the IPv6 aggregation route. Use the **no** form of this command to delete the aggregation route.

summary-prefix *ipv6-prefix/prefix-length* [**level-1** | **level-2** | **level-1-2**]

no summary-address *ipv6-prefix/prefix-length*

Parameter Description

Parameter	Description
<i>ipv6-prefix / prefix-length</i>	Aggregation network address and the IP prefix length of the aggregation network address.
level-1	Applies to the Level-1 only.
level-2	Applies to the Level-2 only.
level-1-2	Applies to both Level-1 and Level-2.

Defaults

By default, no aggregation route is configured.

Command Mode

Address-family ipv6 mode

Usage Guide

With the aggregation route configured, if there is any reachable address or reachable network segment route in the aggregation route, it will publish the aggregation route instead of the detailed route.

Configuration Examples

```
QTECH(config)# router isis
QTECH(config-router)# address-family ipv6
QTECH (config-router-af)# summary-prefix 1000::/96 level-1-2
```

Related Commands

Command	Description
summary-address	Configures the IPv4 aggregation route.

Platform Description

N/A

4.66. two-way-maintain

Use this command to enable the IS-IS two-way maintenance function.

Use the **no** form of this command to disable the IS-IS two-way maintenance function.
no two-way-maintain

Parameter Description

Parameter	Description
N/A	N/A

Defaults Mode

The IS-IS two-way maintenance function is enabled by default.

Default Level

14

Usage Guide

In a large-scale network, a large number of packets are sent and received, which occupies lots of CPU and memory resources, causing the delay or discarding of some IS-IS packets. If the time required for processing hello packets exceeds the neighbor relationship maintenance duration, the corresponding neighbor relationship times out and is removed. When the two-way maintenance function is enabled, if a large number of packets exist on the network, the LSP packets, CSNP packets, and PSNP packets from a neighbor in addition to hello packets can also be used to maintain the two-way relationship with the neighbor, preventing the neighbor failure caused by delay or discarding of hello packets.

Configuration Examples

The following example disables the IS-IS two-way maintenance function.

```
QTECH(config)# router isis 1
QTECH(config-router)# no two-way-maintain
```

4.67. virtual-system

Parameter Description

Use this command to configure an additional system ID for fragment extension. Use the **no** form of this command to remove the additional system ID.

virtual-system *system-id*

no virtual-system *system-id*

Defaults No additional system ID is configured by default.

Parameter	Description
<i>system-id</i>	Additional system ID. The length is 6 bytes.

Command Mode

IS-IS routing process configuration mode

Usage Guide

Use this command to configure an additional system ID for LSP fragment extension.

The system must be enabled with fragment extension mode and configured with the additional system ID to enable LSP fragment extension.

Configuration Examples

The following example configures an additional system ID for fragment extension.

```
QTECH(config)# router isis
QTECH(config-router)# virtual-system 0000.0000.0034
```

Related Commands

Command	Description
N/A	N/A

Description

3.1 vrf

Parameter Description

Use this command to bind the ISIS process with a VRF instance. Use the **no** form of this command to unbind the IS-IS process from the VRF instance.

vrf *vrf-name*

no vrf *vrf-name*

Parameter	Description
<i>vrf-name</i>	VRF instance name. The VRF instance must be configured.

Defaults

No IS-IS process is bound with the VRF instance.

Command Mode

IS-IS routing process configuration mode

Usage Guide

Before you configure this command, the specified VRF instance must be configured. If you want to build the IS-IS v6 neighbor, the multi-protocol VRF and IPv6 protocol must be enabled.

The following restrictions are for binding IS-IS process with VRF instance:

The IS-IS process in the same non-default VRF instance must be configured with a different system ID. The IS-IS process in the different VRF instance can be configured with the same system ID.

An IS-IS process can be bound with only one VRF instance. A VRF instance can be bound with multiple IS-IS processes.

If a VRF instance bound with an IS-IS changes, the IS-IS enabled interfaces which are bound with the VRF instance and the redistribute configuration in IS-IS routing process configuration mode will be removed.

Configuration Examples

The following example binds an IS-IS process with a VRF instance.

```
QTECH(config)#vrf definition vrf_1 QTECH(config-vrf)#address-family ipv4
QTECH(config-vrf-af)#exit-address-family

QTECH(config)# router isis QTECH(config-router)# vrf vrf_1
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

4.68. show clns is-neighbors

Use this command to display all IS neighbors to provide the adjacency relationship of routers.

show clns [tag] is-neighbors [interface-type interface-number] [detail]

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.
<i>interface-type</i> <i>interface-number</i>	Specifies the name of interface.
detail	Displays detailed information of all interfaces.

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide

N/A

Configuration Examples

The output results of the **show clns is-neighbors detail** command are displayed as below:

```
Area (null):
System Id Type      IP Address      State   Holdtime Circuit Interface
ID: 1    L1    1.0.0.2    Up      9    r1.01
L2    1.0.0.2.    0      9      r1.01
Adjacency
Uptime: 00:00:54
Area Address(es): 49.1111

SNPA: 00d0. f8bc. de08

IPv6 Address(es): fe80::2a9:15ff:fe36:5413 Level-1 MTID: Standard
```

Related Commands

Command	Description
show clns neighbors	Displays all IS neighbors to provide the router information and the adjacency relationship of terminal system.

Platform Description

N/A

4.69. show clns neighbors

Use this command to display all IS neighbors to provide the router information and the adjacency relationship of terminal system.

show clns [*tag*] **neighbors** [*interface-type interface-number*] [**detail**]

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.
<i>interface-type</i> <i>interface-number</i>	Specifies the name of the interface.
detail	Displays detailed information of all interfaces.

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example displays all IS neighbors to provide the router information and the adjacency relationship of terminal system.

```
QTECH# show clns neighbors detail
```

```
Area (null):
```

```
System Id      SNPA      State  Holdtime  Type
Protocol      Interface r1      00d0.f8bc.de08  Up      7      L1      IS-IS
GigabitEthernet 0/0
Up      9      L2      IS-IS      GigabitEthernet 0/0
```

```
Adjacency ID: 1
```

```
Uptime: 00:01:40
```

```
Area Address(es): 49.1111 IP Address(es): 1.0.0.2
```

```
IPv6 Address(es): fe80::2a9:15ff:fe36:5413 Level-1 MTID: Standard
```

```
Level-2 MTID: Standard
```

```
Level-1 Protocols Supported: IPv4, IPv6
```

Related Commands

Command	Description
show clns is-neighbors	Displays all IS neighbors to provide the router adjacency relationship.

Platform Description

N/A

4.70. show isis counter

Use this command to display various statistics of IS-IS.

show isis [tag] counter

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide **N/A**

Configuration Examples

```
QTECH# show isis counter
Area (null):
IS-IS Level-1 isisSystemCounterEntry: isisSysStatCorrLSPs:
```

The output results of the **show clns neighbors details** are displayed as below:

```
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmpToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.71. show isis database

Use this command to display the LSP database.

show isis [*tag*] **database** [*FLAGS* | *LEVEL* | *LSPID*]

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.

<i>FLAGS</i>	<p>The format is displayed as below:</p> <p>detail verbose</p> <p>detail: detailed information</p> <p>Verbose: more detailed information than the detail.</p>
<i>LEVEL</i>	<p>The format is displayed as below:</p> <p>I1 I2 level-1 level-2</p> <p>I1 and level-1: specify the LSP database of the Level-1. I2 and level-2: specify the LSP database of the Level-2</p>
<i>LSPID</i>	<p>Specifies the ID number of LSP to show the corresponding LSP information only.</p>
<i>tag</i>	<p>Specifies the IS-IS instance.</p>

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide

N/A

```
QTECH# show isis database detail
Area (null):
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num LSP Checksum LSP Holdtime
NLPID:         0xCC
Hostname:      QTECH
IP Address:    1.0.0.1
               IS r1.01
               IP 1.0.0.0 255.255.255.0
               ATT/P/OL
QTECH.00-00 * 0x00000007 0xCDD5 1011 0/0/0
  Area Address: 49.1111
Metric: 10
Metric: 10
r1.00-00 0x00000006 0xA771 1032 0/0/0
Area Address: 49.1111
```

```

NLPID:      0xCC
Hostname:    r1
IP Address:  1.0.0.2

                IS r1.01
                IP 1.0.0.0 255.255.255.0
0          IS r1.00
0          IS QTECH.00
NLPID:      0xCC
Hostname:    QTECH
IP Address:  1.0.0.1
Metric:      10      IS r1.01
Metric:      10      IP 1.0.0.0 255.255.255
r1.01-00    0x00000002    0xA771    1032    0/0/0/

Metric:      10
Metric:      10

r1.01-00    0x00000002    0x062A    989    0/0/0

Metric:      10
Metric:      10

IS-IS Level-2 Link State Database:

  LSPID LSP Seq Num LSP Checksum      LSP Holdtime  ATT/P/OL
QTECH.00-00 * 0x0000000A 0xC7D8      1033          0/0/0

  Area Address: 49.1111

```

Configuration Examples

The output results of the `show isis database detail` command are displayed as below:

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.72. show isis graceful-restart

Use this command to display the status information related to the IS-IS GR.

show isis [tag] graceful-restart

Parameter Description

Parameter	Description
<i>tag</i>	IS-IS instance name

Defaults

N/A

Command Mode

Privileged EXEC mode/ global configuration mode/ interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the GR information of the IS-IS

```
QTECH(config)# show isis graceful-restart
```

```
Area (null):
Graceful-restart Helper: enabled
Level 1:
  GigabitEthernet 0/0: RR received: 0
Level 2:
  GigabitEthernet 0/0: RR received: 0
Graceful-restart: enabled
Graceful-period: 400s, Level timer: 60s, Interface timer: 3s
Instance GR status: not restarting
```

Related Commands

Command	Description
graceful-restart	Enables the IS-IS GR Restart capability.
graceful-restart grace-period	Configures the maximum interval of the graceful-restart.
graceful-restart helper disable	Disables the IS-IS GR Help

	capability.
graceful-restart	Enables the IS-IS GR Restart capability.

Platform Description

N/A

4.73. show isis hostname

Use this command to display the mapping relation between the router name and system ID.

show isis [*tag*] **hostname**

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.

Defaults

N/A

Command Mode

Privileged EXEC mode/ global configuration mode/ interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH# show isis hostname
```

```
System ID Dynamic Hostname Area (null)
```

```
* 5555.5555.5555 QTECH
```

```
1111.1111.1111 R1
```

```
System ID Dynamic Hostname Area 1
```

```
* 4444.4444.4444 QTECH
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.74. show isis ipv6 topology

Use this command to display information about the IPv6 unicast topology to which an IS-IS router is connected.

show isis [*tag*] **ipv6 topology** [*I1* | *I2* | **level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>tag</i>	IS-IS instance
I1	Topology of a specified Level-1 router
level-1	Topology of a specified Level-1 router
I2	Topology of a specified Level-2 router
level-2	Topology of a specified Level-2 router

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example displays the IPv6 unicast topology information.

```
QTECH#show isis ipv6 topology
Area (null):
IS-IS paths to level-1 routers
System Id Metric Next-Hop SNPA Interface
r1      10      r1      00d0.f822.33ad GigabitEthernet 0/0 QTECH
IS-IS paths to level-2 routers
System Id Metric Next-Hop SNPA Interface
r1      10      r1      00d0.f822.33ad GigabitEthernet 0/0 QTECH --
```

Field description:

Field	Description
Area	Instance tag
System Id	System ID
Metric	Metric value
Next-Hop	Next hop
SNPA	SNPA address
Interface	Interface name

4.75. show isis interface

Use this command to display the information about IS-IS interface.

show isis [*tag*] **interface** [*interface-type interface-number*] [*counter*]

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance name.
<i>interface-type</i> <i>interface-number</i>	Specifies the Interface name.

Command Mode

Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example displays the IS-IS interface.

```
QTECH# show isis interface
Area (null):
VLAN 1 is up, line protocol is up Routing
  Protocol: IS-IS ((null))
    Network Type: Broadcast Circuit Type:
    level-1-2 Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000001 Local SNPA:
    00d0.f822.33ab
    IP interface address:
    1.0.0.1/24
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: r1.01

    Level-1 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s, Retransmit:5s

    Level-1 LSPs in queue: 0 Level-1 LSPs

    flood: 5

    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: r1.01

    Level-2 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s, Retransmit:5s

    Level-2 LSPs in queue: 0 Level-2 LSPs

    flood: 5

    Number of active level-2 adjacencies: 1 Next IS-IS LAN
    Level-1 Hello in 5 seconds Next IS-IS LAN Level-2 Hello
    in 5 seconds BFD Enabled (Anti-congestion)
    Eligible to backup traffic
QTECH# show isis interface counter
```

The following example displays the statistics of the IS-IS interface.

```
Area (null): GigabitEthernet 1/1/0:
  IS-IS LAN Level-1 isisCircuitCounterEntry:
    isisCircAdjChanges: 4
```

```
isisCircNumAdj: 2
isisCircInitFails: 0
isisCircRejAdjs: 0
isisCircIDFieldLenMismatches: 0
isisCircMaxAreaAddrMismatches: 0
isisCircAuthTypeFails: 0
isisCircAuthFails: 0
isisCircLanDesISChanges: 1
IS-IS LAN Level-2 isisCircuitCounterEntry:
isisCircAdjChanges: 4
isisCircNumAdj: 2
isisCircInitFails: 0
isisCircRejAdjs: 0
isisCircIDFieldLenMismatches: 0
isisCircMaxAreaAddrMismatches: 0
isisCircAuthTypeFails: 0
isisCircAuthFails: 0
isisCircLanDesISChanges: 1
IS-IS Level-1 isisPacketCounterEntry:
isisPacketCountIIHello in/out: 187/278
isisPacketCountLSP in/out: 10/7
isisPacketCountCSNP in/out: 0/92
isisPacketCountPSNP in/out: 0/0
isisPacketCountUnknown in/out: 0/0
IS-IS Level-2 isisPacketCounterEntry:
isisPacketCountIIHello in/out: 186/286
isisPacketCountLSP in/out: 17/9
isisPacketCountCSNP in/out: 1/91
isisPacketCountPSNP in/out: 0/0
isisPacketCountUnknown in/out: 0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.76. show isis mesh-groups

Use this command to display the mesh-group configurations on each interface.

show isis [tag] mesh-groups

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.

Defaults

N/A

Command Mode

Usage Guide

Configuration Examples

Privileged EXEC mode, global configuration mode or interface configuration mode.

N/A

The following example displays the mesh groups.

```
QTECH# show isis mesh-groups Mesh group
(blocked) FastEthernet 1/1
Mesh group 1 :
FastEthernet 1/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.77. show isis neighbors

Use this command to display the IS-IS neighbors..

show isis [*tag*] **neighbors** [*detail*]

Parameter Description

Parameter	Description
<i>tag</i>	Displays the IS-IS instance.
<i>detail</i>	Displays the detailed information of all interfaces.

Defaults

N/A

Mode

Usage Guide

N/A

Configuration Examples

The following example displays details of IS-IS neighbors.

```
QTECH# show isis neighbors detail
```

```
Area (null):
```

```
System Id Type IP Address State Holdtime Circuit Interface
```

```
r1          L1... 1.0.0.2      Up      9          r1.01    GigabitEthernet 0/0
```

```
          L2   1.0.0.2      Up      9          r1.01    GigabitEthernet 0/0
```

```
Adjacency ID: 1
```

```
Uptime: 00:06:25
```

```
Area Address(es) 49.1111
```

```
SNPA: 00d0.f8bc.de08
```

```
IPv6 Address(es): fe80::2a9:15ff:fe36:5413 Level-1 MTID:
```

```
Standard
```

```
Level-2 MTID: Standard
```

```
Level-1 Protocols Supported: IPv4, IPv6
```

```
Level-2 Protocols Supported: IPv4, IPv6 BFD(IPv4) session
```

```
state: Up
```

```
BFD(IPv6) session state: Up
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.78. show isis virtual-neighbors

Use this command to display the virtual system neighbor information of an IS-IS system.

show isis [tag] virtual-neighbors

Parameter Description

Parameter	Description
<i>tag</i>	<i>IS-IS instance.</i>

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH# show isis virtual-neighbors
```

```
Area (null):
Virtual System Id      Type      State
1111.1111.1111        L1        DOWN
                      L2        UP
2222.2222.2222        L1        DOWN
                      L2        UP
```

Field description:

Field	Description
Area	Instance tag

Virtual System Id	Virtual system ID
Type	Neighbor type
State	Neighbor status. UP indicates the level at which the extended LSP fragment is created.

4.79. show isis protocol

Use this command to display relevant protocol information about an IS-IS system.

show isis [tag] protocol

Parameter Description

Parameter	Description
tag	IS-IS instance.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example displays relevant protocol information about an IS-IS system.

```
QTECH# show isis protocol IS-IS Router:
(null)
  Binding VRF: vrf Mib-Binding:
  off
  System ID: 0000.0000.0036   IS-type: level-1-2 Virtual
  System ID:
    1111.1111.1111, 2222.2222.2222
  Manual area address(es):
    49.0001, 49.0003
  Interfaces supported by IS-IS: GigabitEthernet 0/0,
    GigabitEthernet 0/1
  Redistributing IPv4:
```

```

isis 1, isis 2 Redistributing IPv6:
isis 3, isis 4
Distance: 115
Generate narrow metrics: Level-1-2 Accept
narrow metrics:           Level-1-2 Generate
wide metrics:             none Accept wide
metrics:                  none
Two-way-maintain: enable

```

Field description:

Field	Description
IS-IS Router	Instance tag
Binding VRF	Name of the VRF bound to the instance
Mib-Binding	Indicates whether the instance is bound with SNMP.
System ID	System ID
IS-type	Level type supported by the instance
Virtual System ID	Extended system ID
Manual area address(es)	Area ID
Interfaces supported by IS-IS	Interface associated with the instance
Redistributing IPv4	Source of redistributed IPv4 routes
Redistributing IPv6	Source of redistributed IPv6 routes
Distance	IS-IS management weight
Generate narrow metrics	Type of the generated narrow metrics
Accept narrow metrics	Type of the accepted narrow metrics
Generate wide metrics	Type of the generated wide metrics
Accept wide metrics	Type of the accepted wide metrics
Two-way-maintain	Indicates whether the two-way maintenance

	function is enabled for the instance.
--	---------------------------------------

4.80. show isis topology

Use this command to display the topology of the IS-IS router connection.

show isis [*tag*] **topology** [*WORD* | **all**] [**I1** | **I2** | **level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.
<i>WORD</i>	System ID or host name.
self-originate	Displays the topology of the device.
all	Displays the topology whose root node is the local device or the IS-IS neighbor.
I1	Specifies the topology of Level-1.
level-1	Specifies the topology of Level-1.
I2	Specifies the topology of Level-2.
level-2	Specifies the topology of Level-2.

Defaults

N/A

Command Mode

Privileged EXEC mode/ global configuration mode/ interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays all IS-IS neighbors:

Related Commands

Command	Description
N/A	N/A

```
QTECH#show isis topology
Area (null):
IS-IS paths to level-1 routers
System Id    Metric    Next-Hop    SNPA        Interface
r1           10       r1          00d0.f822.33ad GigabitEthernet 0/0
QTECH      --
IS-IS paths to level-2 routers
System Id    Metric    Next-Hop    SNPA        Interface
r1           10       r1          00d0.f822.33ad GigabitEthernet 0/0
QTECH
```

Platform Description

N/A

5. BGP4 COMMANDS

5.1. address-family ipv4

Use this command to enter IPv4 address family configuration mode to configure BGP configuration mode. Use the **no** or **default** form of this command to exit BGP address configuration mode.

address-family ipv4 [unicast|multicast]

no address-family ipv4 [unicast|multicast] default address-family ipv4 [unicast]

Parameter Description

Defaults

The configuration mode is unicast address prefix by default.

Parameter	Description
unicast	Optional, detailed IPv4 unicast address prefix

Command Mode

BGP configuration mode

Usage Guide

In BGP address configuration mode, use the standard IPv4 address for the configuration. To return to BGP configuration mode, run the command **exit-address-family**.

Configuration Examples

The following example enters the IPv4 address family configuration mode.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# address-family ipv4
```

Related Commands

Command	Description
exit-address-family	Exits the mode.

Platform Description

None

5.2. address-family ipv4 vrf

Use this command to enter the IPv4 VRF address family configuration mode to configure BGP and enable the exchange of route information of a VRF. Use the **no** or **default** form of this command to restore the default setting.

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf-name*

default address-family ipv4 vrf *vrf-name*

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults

No vrf is defined by default.

Command Mode

BGP configuration mode

Usage Guide

You can execute this command to configure or exit the exchange of route information between PEs and CEs.

To return to BGP configuration mode, run the **exit-address-family** command.

If IPv4 VRF and IPv6 VRF address family modes of the same VRF are activated at the same time, and the same neighbor is activated in two address family modes, the neighbor's global commands will be displayed in both address family modes at the same time, while its address family commands will be displayed only under respective address family modes.

Configuration Examples

The following example enters the IPv4 VRF address family configuration mode.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# address-family ipv4 vrf vpn1
```

Related Commands

Command	Description
exit-address-family	Exits the configuration mode.

Platform Description

N/A

5.3. address-family ipv6

Use this command to enter IPv6 address family configuration mode and enable the exchange of IPv6 route information. Use the **no** or **default** form of this command to restore the default setting. Use the **exit-address-family** command to exit BGP address-family configuration mode.

address-family ipv6 [unicast]

no address-family ipv6 [unicast] default address-family ipv6 [unicast]

Parameter Description

Defaults

The configuration mode is unicast address prefix by default.

Parameter	Description
unicast	Optional, enters IPv6 unicast address-family configuration mode.

Command Mode

BGP configuration mode or BGP Scope configuration mode

Usage Guide

You can use this command not only to enter IPv6 address-family configuration mode of the BGP to configure the IPv6 neighbors, but also activate neighbors in IPv6 address-family configuration mode after configuring IPv6 neighbors in BGP configuration mode.

The **exit-address-family** command is used to return to BGP configuration mode.

Configuration Examples

The following example enters the IPv6 address family configuration mode.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# address-family ipv6
```

Related Commands

Command	Description
exit-address-family	Exits the mode.

Platform Description

None

5.4. address-family ipv6 vrf

Use this command to enter BGP configuration mode, enable the IPv6 route information exchange function under a vrf. Use **no** or **default** form of this command to restore the default setting. Use the **exit-address-family** command to exit BGP address configuration mode.

address-family ipv6 vrf *vrf-name*

no address-family ipv6 vrf *vrf-name*

default address-family ipv6 vrf *vrf-name*

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults

No vrf address family is defined by default.

Command Mode

BGP configuration mode

Usage Guide

You can use this command to start configuring (or quit) the exchange of BGP route information between PE or MCE device and CE.

You can use the **exit-address-family** command to return to BGP configuration mode.

If ipv4 vrf and ipv6 vrf address family modes of the same vrf are activated at the same time, and same neighbor is activated in two address family modes, the neighbor's global commands will be displayed in both the address family modes at the same time, while its address family commands will only be displayed under respective address family mode.

Configuration Examples

The following example enters the IPv6 VRF address family configuration mode.

```
QTECH(config)# router bgp 65000
```

Configuration Examples

Platform Description

```
QTECH(config-router)# address-family ipv6 vrf vpn1
```

Command	Description
---------	-------------

exit-address-family	Exits the mode.
----------------------------	-----------------

N/A

5.5. address-family l2vpn

Use this command to enter the L2VPN address family configuration mode and enable the exchange of L2VPN route information between BGP neighbors. Use the **no** or **default** form of this command to restore the default settings.

address-family l2vpn {evpn}

no address-family l2vpn {evpn } default address-family l2vpn {evpn }

Parameter Description

Parameter	Description
evpn	L2VPN EVPN address family.

Defaults

No L2VPN address family is defined by default.

Command Mode

BGP configuration mode / BGP scope global configuration mode

Usage Guide

Use the **exit-address-family** command to exit the L2VPN address family configuration mode.

Configuration Examples

The following example enters the L2VPN VPLS address family configuration mode.

```
QTECH(config)# router bgp 100
QTECH(config-router)# address-family l2vpn vpls
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.6. advertise ipv4 unicast

Use this command to configure IPv4 VRF re-distribution. Use the **no** form of this command to disable the IPv4 VRF re-distribution. Use the **default** form of this

command to restore the default settings.

advertise ipv4 unicast no advertise ipv4 unicast

default advertise ipv4 unicast

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The IPv4 VRF re-distribution function is disabled by default.

Command Mode

BGP L2VPN EVPN address family mode.

Usage Guide

Limitations on re-distribution of IPv4 unicast routes into BGP:

- The re-distribution of IPv4 unicast routes into BGP function can only take effect in BGP L2VPN EVPN address family mode.
- Only after the VXLAN module has advertised the L3 virtual MAC address, the IPv4 unicast routes can be re-distributed.
- Only after the route-target import attribute of EVI instance matches the route-target attribute of VRF, the IPv4 unicast routes can be re-distributed.
- The non-VRF IPv4 unicast routes cannot be re-distributed.

Configuration Examples

The following example configures the re-distribution of IPv4 unicast routes into BGP.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# address-family l2vpn evpn QTECH(config-
router-af)# advertise ipv4 unicast
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.7. advertise ipv6 unicast

Use this command to configure IPv4 VRF re-distribution. Use the **no** form of this command to disable the IPv4 VRF re-distribution. Use the **default** form of this command to restore the default settings.

Parameter Description

no advertise ipv6 unicast default advertise ipv6 unicast

Parameter	Description
N/A	N/A

Defaults

The IPv6 VRF re-distribution function is disabled by default.

Command Mode

BGP L2VPN EVPN address family mode.

Usage Guide

Limitations on re-distribution of IPv6 unicast routes into BGP:

The re-distribution of IPv6 unicast routes into BGP function can only take effect in BGP L2VPN EVPN address family mode.

Only after the VXLAN module has advertised the L3 virtual MAC address, the IPv6 unicast routes can be re-distributed.

Only after the route-target import attribute of EVI instance matches the route-target attribute of VRF, the IPv6 unicast routes can be re-distributed.

The non-VRF IPv6 unicast routes cannot be re-distributed.

Configuration Examples

The following example configures the re-distribution of IPv6 unicast routes into BGP.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# address-family l2vpn evpn QTECH(config-
router-af)# advertise ipv6 unicast
```

Related Commands

Platform Description

Command	Description
N/A	N/A

N/A

5.8. aggregate-address (IPv4)

Use this command to set the aggregate IPv4 route. Use the **no** or **default** form of this command to restore the default setting.

aggregate-address *ip-address mask* [**as-set**] [**summary-only**] [**attribute-map** *map-tag*]
no aggregate-address *ip-address mask*
default aggregate-address *ip-address mask*

Parameter Description

Parameter	Description
<i>ip address</i>	IP address of the aggregate route
<i>mask</i>	Mask of the aggregate route
as-set	Keeps the AS path information of the path in the aggregate address range.
summary-only	Advertises only the aggregate route.
attribute-map	Configures the routing policy to control the route attribute.
<i>map-tag</i>	Route map name. Up to 32 characters is allowed.

Defaults

The address aggregation is not configured by default.

Command Mode

BGP configuration mode, IPv4 address family configuration mode, or IPv4 VRF address family configuration mode

Usage Guide

The BGP-enabled device will advertise all path information both before and after aggregation by default. Use the **aggregate-address summary-only** command to advertise the aggregate route only.

Configuration Examples

The following example sets the aggregate IPv4 route.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# aggregate-address 10.0.0.0
255.0.0.0 as-set
```

Related Commands

Command	Description
---------	-------------

router bgp	Enables the BGP protocol.
-------------------	---------------------------

Platform Description

None

5.9. bgp advertise non-transitive extcommunity

Use this command to allow carried non-transitive extcommunity when BGP is notifying EBGp neighbors of a route. Use the **no** or **default** form of this command to restore the default setting. **bgp advertise non-transitive extcommunity**

no bgp advertise non-transitive extcommunity default bgp advertise non-transitive extcommunity

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Non-transitive extcommunity is removed when notifying EBGp neighbors of a route.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

By default, when notifying EBGp neighbors of a route, neighbors will not be notified of extcommunity with the "non-transitive" flag. This configuration can enable the notification of non-transitive extcommunity.

Non-transitive extcommunity will be carried when notifying alliance EBGp or IBGP neighbors of a route.

Configuration Examples

The following example allows carried non-transitive extcommunity.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp advertise non-transitive extcommunity
```

Configuration Examples

Command	Description
---------	-------------

router bgp	Enables BGP protocol.
-------------------	-----------------------

Platform Description

N/A

5.10. bgp always-compare-med

Use this command to compare Multi Exit Discriminator (MED) all the time. Use the no or default form of this command to restore the default setting.

bgp always-compare-med no bgp always-compare-med

default bgp always-compare-med

Parameter Description

Parameter	Description
N/A	N/A

Defaults

MED of peer paths from the same AS is compared by default.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

The MED value is compared for paths of peers from the same AS by default. This command can be used to allow comparing MED values for paths from different ASs. If there are multiple valid paths to the same destination, the one with lower MED value has higher priority.

This command is not recommended unless you are sure that different ASs are using the same IGP and routing method.

Configuration Examples

The following example compares Multi Exit Discriminator (MED) all the time.

```
QTECH(config)# router bgp 65000
```

```
QTECH(config-router)# bgp always-compare-med
```

Related Commands

Command	Description
show ip bgp	Displays the BGP route entry.

bgp bestpath med confed	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med missing-as-worst	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform Description

None

5.11. bgp asnotation dot

Use this command to modify the displaying mode of the 4-byte AS notation and the matching type of the regular expression as the dot mode (that is, two dotted decimal numbers). Use the no or default form of this command to restore the default setting.

bgp asnotation dot no bgp asnotation dot

default bgp asnotation dot

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The 4-byte AS notation is shown in decimal digit, and the regular expression also matches the 4-byte AS notation with decimal digit by default.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

Our devices support two modes of representing the 4-byte AS notation. One is decimal digit, and the other one is dot mode which represents the 65536 with 1.0. The decimal format is same as the default format, which represents the 4-byte AS notation with decimal digits. The dot mode displays the 4-byte AS notation in the format of ([two high bytes.] two low bytes). If the [two high bytes.] is zero, it will not be displayed. That is, the AS notation

represented as 65536 in decimal is 1.0 in the dot mode. In another example, the AS notation is 65534 represented in decimal, while it is represented as 65534 in the dot mode without the zero in front.

No matter which mode will be adopted to display the 4-byte AS notation, both modes can be used when entering the configuration commands. But the representation and displaying mode of the

4-byte AS notation in the regular expression must be the same. Otherwise, the matching will fail. After executing the `bgp asnotation` command, you must use the `clear ip bgp *` to perform the resetting, so as to re-match the filtering condition of the regular expression.

The AS notation is represented as 1 to 65535 no matter using decimal or dot mode.

Configuration Examples

The following example modifies the showing mode of the 4-byte AS notation.

```
QTECH(config)# router bgp 1.0
QTECH(config-router)# bgp asnotation dot
```

Related Commands

Command	Description
show ip bgp summary	Displays the related information of BGP neighbor.

Platform Description

None

5.12. bgp bestpath as-path ignore

Use this command to disregard the length of the AS path. Use the **no** or **default** form of this command to restore the default setting.

`bgp bestpath as-path ignore no bgp bestpath as-path ignore`

default bgp bestpath as-path ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The AS path length is considered in choosing the optimal path by default.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

BGP will not take the length of the AS path into account when it selects the optimal path as specified in RFC1771. In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path into account when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.

Configuration Examples

The following example disregard the length of the AS path.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp bestpath as-path ignore
```

Related Commands

Command	Description
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.13. bgp bestpath as-path multipath-relax

Use this command to enable AS path multipath-relax (only comparing the AS path length) for BGP multipathing load. Use the no or default form of this command to restore the default setting.

```
bgp bestpath as-path multipath-relax no bgp bestpath as-path multipath-relax
default bgp bestpath as-path multipath-relax
```

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

BGP requires that AS path attributes must be the same when calculating equal-cost multipath (ECMP) by default.

Defaults

BGP configuration mode / Scope global configuration mode

Usage Guide

BGP compares AS path attributes in a precise way when selecting the optimal path as ECMP by default. Only paths with same AS path attributes can constitute equal-cost paths.

As a result, BGP multipathing load balancing cannot be implemented in an application scenario. After AS path multipath-relax is enabled, only the AS path length is compared, allowing the implementation of BGP multipathing load balancing.

Configuration Examples

The following example enables AS path multipath-relax for BGP multipathing load.

```
QTECH(config)# router bgp 65530
```

```
QTECH(config-router)# bgp bestpath as-path multipath-relax
```

Related Commands

Command	Description
router bgp	Enables BGP.
show ip bgp	Displays BGP routing entries.

Platform Description

None

5.14. bgp bestpath compare-confed-aspath

Use this command to compare the AS path length of the confederation from the same external routes when selecting the optimal path, with smaller AS path in the confederation for higher path priority. Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

Defaults

bgp bestpath compare-confed-aspath no bgp bestpath compare-confed-aspath

default bgp bestpath compare-confed-aspath

Parameter	Description
N/A	N/A

The AS path of the EBGp peer routes inside the same confederation is not compared by default when selecting the optimal path. Instead, the routing method is implemented.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

During the selection of the same routing information from the peer of the internal EBGP By default, the AS path of the confederation is not compared. This command is used to compare the AS path of the confederation.

Note that if a route contain no AS path of the confederation, it is impossible to implement the AS path comparison for that route.

Configuration Examples

The following example compares the AS path length of the confederation.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp bestpath compare-confed-aspath
```

Related Commands

Command	Description
show ip bgp	Displays the BGP route entry.
bgp router-id	Sets the BGP Device ID.

Platform Description

None

5.15. bgp bestpath compare-routerid

Use this command to compare the router ID of the same external routes when selecting the optimal path, with smaller router ID for higher path priority. Use the no or default form of this command to restore the default setting.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid default bgp bestpath compare-routerid

Parameter Description

Parameter	Description
N/A	N/A

Defaults

If two paths received from different EBGP peers have the same path, the first one is considered with higher priority by default.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

If two paths with identical path attributes are received from different EBGP peers during the selection of the optimal path, we will select the optimal path according to the sequence of

receiving the paths by default. You can select the path with smaller Device ID as the optimal path by configuring the following commands.

Configuration Examples

The following example compares the router ID of the same external routes.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp bestpath compare-routerid
```

Related Commands

Command	Description
show ip bgp	Displays the BGP route entry.
bgp router-id	Sets the BGP Device ID.

Platform Description

None

5.16. bgp bestpath med confed

Use this command to compare the MED value of the path of the internal peer from AS confederation during selecting the optimal path. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath med confed [missing-as-worst] no bgp bestpath med confed [missing-as-worst]

default bgp bestpath med confed [missing-as-worst]

Parameter Description

Parameter	Description
missing-as-worst	Sets the priority of the path without MED attribute as the lowest.

Defaults

The MED value of the path of the peer inside the AS confederation is not compared by default when selecting the optimal path.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

The MED attribute of the path is transferred between the ASs inside the confederation. You may set always comparing this value.

Configuration Examples

The following example compares the MED value of the path of the internal peer.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp bestpath med confed
```

Related Commands

Command	Description
show ip bgp	Displays the BGP route entry.
bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med missing-as-worst	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform Description

None

5.17. bgp bestpath med missing-as-worst

Use this command to set the priority of the path without MED attribute as the lowest when selecting the optimal path. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath med missing-as-worst no bgp bestpath med missing-as-worst
default bgp bestpath med missing-as-worst

Parameter Description

Parameter	Description
N/A	N/A

Defaults

If a path without MED attribute is received, the MED value of the path is 0 by default. Such route has the highest priority according to the above-mentioned rule.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

The MED value of a path without MED attribute will be 0 by default. For the smaller the MED value, the higher the priority of the path is, the MED value of this path has the highest priority. This command can be used to figure the path without MED attribute has the lowest priority.

Configuration Examples

The following example sets the priority of the path without MED attribute as the lowest.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp bestpath medmissing-as-worst
```

Related Commands

Command	Description
show ip bgp	Displays the BGP route entry.
bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med confed	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform Description

None

5.18. bgp bestpath multipath-compare-routerid

Use this command to enable the router ID comparison among multiple BGP paths. Load balancing can be implemented only when multiple paths (same router ID) are from the same device. Use the **no** form of this command to disable the router ID comparison among multiple BGP paths. Use the **default** form of this command to restore the default settings.

bgp bestpath multipath-compare-routerid no bgp bestpath multipath-compare-routerid

default bgp bestpath multipath-compare-routerid

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The router ID comparison among multiple BGP paths is disabled by default.

Command Mode

BGP configuration mode, BGP Scope Global Configuration Mode

Default Level

14

Usage Guide

N/A

Configuration Example

The following example enables the router ID comparison among multiple BGP paths.

Verification

Run the **show running-config** command to display the BGP configuration.

```
QTECH(config)# router bgp 65000
```

```
QTECH(config-router)# bgp bestpath multipath-compare-routerid
```

5.19. bgp client-to-client reflection

Use this command to enable the route reflection function between clients on the device.
Use the **no** or

default form of this command disables the route reflection function between clients.

bgp client-to-client reflection

no bgp client-to-client reflection default bgp client-to-client reflection

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled without the client for route reflection by default.

Command Mode

Usage Guide

In general, it is unnecessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the route among clients.

However, if the full connection relationship is established for all clients, the function for the route reflector to reflect the client route can be disabled.

To disable the route reflection function, use the command **no bgp client-to-client reflection**.

Configuration Examples

The following example shows how to enable the route reflection function between clients on the device.

```
QTECH(config)# router bgp 65000
```

```
QTECH(config-router)# no bgp client-to-client reflection
```

Related Commands

Command	Description
bgp cluster-id	Configures the cluster ID of the route reflector.
neighbor route-reflector-client	Configures the client of the route reflector and configure itself as the route reflector.

Platform Description

None

5.20. bgp cluster-id

Use this command to configure the cluster ID of the route reflector. Use the **no** or **default** form of this command to restore it to the default setting.

bgp cluster-id *cluster-id*

Parameter Description

no bgp cluster-id default bgp cluster-id

Parameter	Description
<i>cluster-id</i>	Cluster ID of the route reflector, an IP address of up to four bytes or an integer (must be entered in

	form of IP address)
--	---------------------

Defaults

The cluster id is the router-id of the route reflector by default.

Command Mode

BGP configuration mode / Scope global configuration mode

Usage Guide

In general, one group is only configured with one route reflector. In this case, the Device ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.

Configuration Examples

The following example configures the cluster ID of the route reflector.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp cluster-id 10.0.0.1
```

Related Commands

Command	Description
bgp client-to-client reflection	Configures the route reflection between clients.
neighbor route-reflector-client	Configures the client of the route reflector and configures itself as the route reflector.

Platform

Description

None

5.21. bgp confederation identifier

Use this command to configure the AS confederation identifier. Use the no or default form of this command to restore the default setting.

bgp confederation identifier *as-number*

no bgp confederation identifier default **bgp confederation identifier**

Parameter Description

Parameter	Description
as-number	AS confederation identifier in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, which is represented as 1 to 65535.65535 in dot mode.

Defaults

There is no confederation identifier by default

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

The confederation is a measure to reduce the connections of IBGP peers within the AS.

One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.

Configuration Examples

Related Commands

The following example configures the AS confederation identifier.

```
QTECH(config-router)# bgp confederation identifier 65000
```

Command	Description
bgp confederation peers	Adds member AS of the AS confederation.

Platform Description

None

5.22. bgp confederation peers

Use this command to configure member ASs of the AS confederation. Use the **no** or **default** form of this command to restore the default setting.

bgp confederation peers *as-number* [...*as-number*]

no bgp confederation peers *as-number* [...*as-number*]

default bgp confederation peers [*as-number* [...*as-number*]]

Parameter Description

Parameter	Description
<i>as-number</i>	Member ASs in the confederation range from 1 to 65535. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.

Defaults

There is no confederation member by default.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

The confederation is a measure to reduce the connections of BGP peers within the AS.

One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. The whole external confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.

This command is used to specify the member AS of a confederation.

This command can configure up to 25 members of a confederation at one time. For more members, enter them for several times.

Configuration Examples

Related Commands

The following example configures member ASs of the AS confederation.

```
QTECH(config-router)# bgp confederation peers 6500065100
```

Command	Description
bgp confederation identifier	Configures the confederation identifier.

Platform Description

None

5.23. bgp dampening

Use this command to enable the routing attenuation and set the attenuation parameters in the address-family or routing configuration mode. Use the **no** or **default** form of this command to restore the default setting.

bgp dampening [*half-life* [*reusing suppressing duration*] | **route-map** *name*]

no bgp dampening default bgp dampening

Parameter Description

Parameter	Description
half-life	Half-life period, ranging from 1 to 45 minutes
reusing	When the penalty value reaches this value, the routing suppression is cancelled. The value ranges from 1 to 10000.
suppressing	When the penalty value reaches this value, routing is suspended. The value ranges from 1 to 20000.
duration	Maximum time for routing suppression, ranging from 1 to 255 minutes
<i>name</i>	Route-map name, apply the routing attenuation to the specified route through the route-map.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4 unicast address-family configuration mode, BGP IPv4 VRF address-family configuration mode, BGP IPv6 unicast address-family configuration mode, BGP IPv6 VRF address-family configuration mode, BGP L2VPN EVPN address-family configuration mode and BGP Scope configuration mode

Usage Guide

The **bgp dampening** command is used to suppress unstable EBGp routes and does not take effect to IBGP routes.

The BGP uses the penalty value to describe the route stability. A larger penalty value indicates a more unstable route. The penalty value increases by 1000 when route oscillation occurs (upon receiving withdraw packets). The penalty value does not increase when the upper limit is reached. The upper limit is determined based on the configured duration value and calculated using the following formula: $\text{Penalty upper limit} = 2^{\text{Duration/Half-life}} \times \text{Reusing}$. In addition, the penalty upper limit cannot be greater than 20000. Therefore, the duration, half-life, and reusing values need to be adjusted based on the network conditions. The relationship among these parameters are as follows:

Half-life \leq Duration

Reusing \leq Suppressing \leq Penalty upper limit

You can also specify only the half-life value. In this case, the duration value is (half-life x 4), the reusing value is 750, and the suppressing value is 2000.

EBGP routes whose penalty value exceeds the suppressing value will be suppressed. Suppressed routes will not be used during BGP route election and will not be advertised to other BGP peers. If route oscillation occurs in suppressed routes, the penalty value will continue to increase until the penalty upper limit is reached.

The penalty value of suppressed routes will decrease by a half each time the half-life time passes. When the penalty value decreases to the reusing value, routes whose attribute is update in the last update will participate in BGP route election again. When the penalty value decreases to 0, routes whose attribute is withdraw in the last update will be deleted from the BGP route table.

Configuration Examples

Related Commands

The following example enables the routing attenuation and set the attenuation parameters.

```
QTECH(config-router)# bgp dampening 30 1500 10000 120
```

Command	Description
clear ip bgp dampening	Clears the BGP suppression and cancels the

	suppression for the routes.
show ip bgp dampening dampened-paths	Displays the suppressed route information.

Platform Description

None

5.24. bgp default ipv4-unicast

Use this command to set the IPv4 unicast address as the default address family. Use the **no** or **default**

form of this command to restore the default setting.

bgp default ipv4-unicast no bgp default ipv4-unicast

default bgp default ipv4-unicast

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The IPv4 unicast address is the default address family.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

This command is used to set the default address family of BGP as the IPv4 unicast address.

Configuration Examples

Related Commands

The following example sets the IPv4 unicast address as the default address family.

QTECH(config-router)#bgp default ipv4-unicast

Command	Description
address-family ipv4	Enters the IPv4 address mode.

Platform Description

None

5.25. bgp default local-preference

Use this command to set the default local-preference attribute value. Use the no or default form of this command to restore the default setting.

bgp default local-preference *value* no bgp default local-preference default bgp default local-preference

Parameter Description

Parameter	Description
<i>value</i>	Local priority attribute, in the range from 0 to 4294967295

Defaults

The local preference value is 100 by default.

Command Mode

BGP configuration mode or BGP Scope configuration mode.

Usage Guide

The BGP takes the local preference as the foundation to compare with the priority of the path learned from IBGP peers. The larger the local preference value, the higher the priority of the path is. The BGP speaker sends the external route received to the IBGP peers to add the local priority value.

Configuration Examples

Command	Description
show ip bgp	Displays the BGP route entry.
bgp always-compare-med	Allows comparing the MED value of the path of the peer from different ASs when electing the optimal path.
bgp bestpath med confed	Allows comparing the MED value of paths of internal peers from AS community when electing the optimal path.
bgp bestpath med	Allows setting the priority of the path without MED attribute

missing-as-worst

as the lowest when electing the optimal path.

Related Commands

The following example sets the default local-preference attribute value.

```
QTECH(config-router)# bgp default local-preference 200
```

Platform Description

None

5.26. bgp default route-target filter

Use this command to enable the route-target filtering. For the VPNv4 routes, filter the community attributes of the route-target by default. Use the **no** or **default** form of this command to disable this function.

```
bgp default route-target filter no bgp default route-target filter
```

```
default bgp default route-target filter
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

BGP configuration mode, VPNv4/VPNv6 address-family configuration mode, BGP L2VPN EVPN address-family configuration mode or BGP Scope Global configuration mode.

Usage Guide

After receiving the VPNv4 route, use the community attributes list of the route-target to filter and distribute different VRFs. With the no form of this command used, the BGP will receive all VPNv4 routes no matter whether these filtered VPNv4 routes will be received by route-target of local VRF.

With the PE route-reflector-client configured for the BGP, the VPNv4 route will not be processed through the route-target filtering. In this case, whether the BGP is enabled, the actions are the same without the route-target filtering.

Configuration Examples

The following example enables the route-target filtering.

```
QTECH(config)# router bgp 65000
```

```
QTECH(config-router)# no bgp default route-target filter
```

Related Commands

Platform Description

Command	Description
neighbor client route-reflector-client	Configures the route-reflector-client, and sets itself as the route reflector.

N/A

3.2 bgp deterministic-med

Use this command to set comparing preferentially the MED values of peer paths from the same AS. By default, the comparison is based on the received order, and the one received the last is compared first. Use the **no** or **default** form of this command to restore the default setting.

```
bgp deterministic med
```

```
no bgp deterministic med default bgp deterministic-med
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

They will be compared with each other according to the sequence the paths are received when the optimal path is selected by default. Execute the following operations in the BGP configuration mode to compare paths of peers from the same AS firstly:

Configuration Examples

Related Commands

The following example sets the comparing preferentially MED values.

```
QTECH(config-router)# bgp deterministic med
```

Command	Description
show ip bgp	Displays the BGP route entry.
bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med confed	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp bestpath med missing-as-worst	Compares paths of peers from the same AS when selecting the optimal path.

Platform Description

None

5.27. bgp enforce-first-as

Use this command to reject the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number. Use the **no** or **default** form of this command to disable this function.

bgp enforce-first-as

no bgp enforce-first-as default bgp enforce-first-as

Parameter Description

Defaults

This function is enabled by default.

Parameter	Description
N/A	N/A

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

The AS number of the device is put into the path section by default to update the update message.

Configuration Examples

Related Commands

The following example rejects the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number.

```
QTECH(config-router)# bgp enforce-first-as
```

Command	Description
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.28. bgp fast-external-fallover

When the network interface used in establishing the connection of the directly-connected EBGP peer fails, use this command to establish the BGP session connection quickly. Use the no or default form of this command to disable this function.

bgp fast-external-fallover

no bgp fast-external-fallover default bgp fast-external-fallover

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

This command takes effect only for the directly-connected EBGP neighbor.

Configuration Examples

Related Commands

The following example creates the fast BGP session.

```
QTECH(config-router)# bgp faster-external-falover
```

Command	Description
router bgp	Enables the BGP protocol.

Platform Description

None

5.29. bgp fast-reroute

Use this command to enable BGP Fast Reroute. Use the **no** or **default** form of this command to restore the default setting.

bgp fast-reroute

no bgp fast-reroute default bgp fast-reroute

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

BGP configuration mode/ BGP IPv4 unicast address family configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP scope global configuration mode.

The BGP Fast Reroute function is supported in the BGP IPv4 unicast address family configuration mode and the BGP IPv4 VRF address family configuration mode.

Usage Guide

Only one backup route will be generated and the next-hop of this backup route cannot be the same as that of the preferred route.

When ECMP is enabled, the FRR cannot generate backup route.

When this function is enabled in the BGP IPv4 VRF address family configuration mode, the priority of BGP FRR is lower than that of VPN FRR. So when the VPN FRR is enabled in IPv4

VRF configuration mode, BGP FRR does not take effect unless VPN FRR is unable to calculate the backup route.

Configuration Examples

The following example enables BGP Fast Reroute.

```
QTECH(config)# router bgp 65530
QTECH(config-router)# bgp faster-reroute
```

Command	Description
N/A	N/A

Platform Description

N/A

5.30. bgp graceful-restart

Use this command to enable the global BGP graceful restart function. Use the no or default form of this command to disable BGP graceful restart.

bgp graceful-restart

no bgp graceful-restart default bgp graceful-restart

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command Mode

By default, BGP graceful restart is enabled so as to help neighbors to perform graceful restart.

BGP configuration mode or BGP Scope Global configuration mode

Guide

The ability is negotiated during initially setting up the connection. So both sides must reach the consistency of the ability. If it is not supported by any side, this router device will perform the GR incorrectly.

With the GR function enabled, the connected Open message will carry the GR ability field to perform the negotiation of the GR ability. To implement the GR correctly, the GR function must be enabled on both sides of the neighbors.

This command does not take effect immediately on all BGP connections that are set up successfully. To negotiate the GR ability immediately, you need to restart the BGP connection

to make the local device negotiate the GR ability with the Peer again by using the clear ip bgp command.

The BGP graceful-restart is used to forward data continuously of the whole network, it requires the device to keep the BGP routing entry valid and forward data continuously when restarting the BGP protocol. Supporting the continuous forwarding during the restarting is related to the hardware ability.

Configuration Examples

The following example enables the graceful restart function of the global BGP.

```
QTECH(config)# router bgp 500
QTECH(config-router)# bgp graceful-restart
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
bgp graceful-restart restart-time	Configures the restart time of the BGP graceful-restart.

Platform Description

N/A

5.31. bgp graceful-restart disable

Use this command to disable GR capability of a BGP address family. Use the **no** or **default** form of this command to restore the default setting.

bgp graceful-restart disable no bgp graceful-restart disable

default bgp graceful-restart disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The function is enabled by default.

Command

BGP configuration mode, IPv4 unicast address family mode, VPNv4 address family mode, VPNv4 configuration mode

Usage Guide

When BGP GR function is enabled, the GR capability for all address families is enabled by default, except for address families that do not support GR capability. After GR capability is enabled, you can use this command in the address family mode to disable the address

family's GR capability. The Configuration of this command in BGP mode is effective on IPv4 Unicast address family.

When BGP GP function is disabled, GR capability is disabled for all address families.

Configuration Examples

The following example disables the graceful restart function of the BGP IPv4 address family.

```
QTECH(config)# router bgp 65000 QTECH(config-router)# bgp graceful-restart QTECH(config-router)# address-family ipv4
QTECH(config-router-af)# bgp graceful-restart disable
```

Configuration Examples

Platform Description

Command	Description
bgp graceful-restart	Enables BGP's GR capability.
address-family ipv4	Enters BGP IPv4 address family mode.

N/A

5.32. bgp graceful-restart restart-time

Use this command to configure the restart time of the BGP graceful-restart. Use the **no** or **default** form of this command to restore the default setting.

bgp graceful-restart restart-time *restart-time*

no bgp graceful-restart restart-time default **bgp graceful-restart restart-time**

Parameter Description

Parameter	Description
<i>restart-time</i>	GR Restarter-hoped longest waiting time before re-establishing the connection between the GR Helper and the GR Restarter, in the range from 1 to 3600 in the unit of seconds.

Defaults

The default is 120.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode.

Usage Guide

The restart time is advertised by GR Restarter to GR Helper, it is GR Restarter-hoped longest waiting time before re-establishing the connection between GR Helper and GR Restarter. After this time, if the BGP connection with GR Restarter is not in Established status, GR Helper will consider

this BGP session failed and will restore the normal BGP. All the routing of the neighbor will be deleted during this period, affecting the data redistribution.

The restart time is advertised in the GR ability field of the BGP Open message. The GR restart time of the two ends of the session is not required to be the same, but it is recommended.

This command does not take effect immediately on all BGP connections that are set up successfully. To advertise the newly set restart time to the GR helper, you need to restart the

BGP connection to negotiate the GR ability again and advertise the restart time by using the `clear ip bgp` command. The configured restart time should not be greater than the Hold Time of the BGP peer, if so, the Hold time will be the restart time when the GR ability is advertised to the BGP peer.

The following example configures the restart time of the BGP graceful-restart.

```
QTECH(config)# router bgp 500 QTECH(config-router)# bgp
graceful-restart
QTECH(config-router)# bgp graceful-restart restart-time 150
QTECH(config-router)# no bgp graceful-restart restart-time
```

Configuration Examples

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform Description

N/A

5.33. bgp graceful-restart stalepath-time

Use this command to configure the time to help the device keep the route valid when executing the BGP graceful-restart. Use the **no** or **default** form of this command to restore the default setting.

`bgp graceful-restart stalepath-time stalepath-time time`

no bgp graceful-restart stalepath-time default bgp graceful-restart stalepath-time

Parameter Description

Parameter	Description
<i>time</i>	Longest time used to keep the stale route valid after restoring the connection with the neighbors, in the range from 1 to 3600 in the unit of seconds

Defaults

The default is 360.

Command Mode

BGP configuration mode

Usage Guide

This command is configured for the parameters of the GR Helper. The stalepath-time is the longest time of the GR Helper waiting to receive the EOR mark of the Restarter after restoring the connection with the GR Restarter. When the GR Helper detects that the connection with the GR Restarter fails, the original route of the Restarter is marked as the “Stale”. However these routes are still used for the routing calculation and forwarding.

The GR Helper updates the routes and cancels the “Stale” mark according to route updating information received from the GR Restarter. If routes marked as “Stale” are not updated in the stalepath-time period, they will be deleted. This mechanism is used to avoid failure in convergence of routes when the GR Helper fails to receive the EOR mark of the GR Restarter for a long time.

The following example configures the restart time of the BGP graceful-restart.

Configuration Examples

```
QTECH(config)# router bgp 500 QTECH(config-router)# bgp
graceful-restart
QTECH(config-router)# bgp graceful-restart stalepath-time 240
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform Description

N/A

5.34. bgp initial-advertise-delay

Use this command to configure the delay period before a BGP device sends its initial updates to peers. Use the no form or default form of this command to restore the default setting.

`bgp initial-advertise-delay delay-time [startup-time]`

`no bgp initial-advertise-delay default bgp initial-advertise-delay`

Use this command to enable the BGP delayed advertisement upon system restart. Thus, the route will be immediately sent after the prefix-list policy is matched. Use the no form or default form of this command to restore the default setting.

`bgp initial-advertise-delay prefix-list prefix-list-name`

`no bgp initial-advertise-delay prefix-list default bgp initial-advertise-delay prefix-list`

Parameter Description

Parameter	Description
<i>delay-time</i>	The delay period, in seconds, before a BGP device sends its updates. The range is from 1 to 600. The default value is 1 second.
<i>startup-time</i>	The time for the BGP device restart. In the period, the neighbor does not send its updates to peers. The range is from 5 to 584,000. The unit is second and the default value is 600 seconds.
<i>prefix-list-name</i>	Name of the prefix-list. It cannot exceed 32 characters.

Defaults

The initial advertisement delay is disabled by default.

Command Mode

BGP configuration mode

Usage Guide

This command is used to configure parameters for delayed neighbor route advertisement during device restart.

delay-time indicates the longest time for sending a route to a neighbor after the BGP neighbor relationship is established. In normal cases, after the neighbor relationship is established, the first route is advertised immediately and subsequent routes are advertised based on the default time. For details, see the `neighbor advertisement-interval` command.

startup-time indicates the configurable startup time and starts to count when the configuration command takes effect. Within the time specified by *startup-time*, routes to

BGP neighbors are advertised periodically based on delay-time. This command can be used to change the route advertisement behavior from the BGP peer to neighbors after device restart.

The prefix-list policy is configured to ensure that partial routes can be normally delivered. The prefix-list policy applies to distributed routes. Matched routes will be normally delivered without being affected by delayed advertisement. For details about the address family scope to which the prefix-list policy applies, see the neighbor prefix-list command.

This command is used by the administrator to adjust the BGP route advertisement behavior during device restart based on the hardware conditions, number of neighbors, number of routes, and actual deployment requirements.

Configuration Examples

The following example configures initial delay to 60 seconds within 500 seconds after BGP restart.

```
QTECH(config)# router bgp 500
```

```
QTECH(config-router)# bgp initial-advertise-delay 60 500
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform Description

N/A

5.35. bgp log-neighbor-changes

Use this command to log the BGP status changes without turning on debug. Use the no or default

form of this command to disable this function.

bgp log-neighbor-changes no bgp log-neighbor-changes

default bgp log-neighbor-changes

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

The debug command can also be used to log BGP status changes. But this command may consume many resources.

Configuration Examples

Related Commands

The following example logs the BGP status changes without turning on debug.

QTECH(config-router)# bgplog-neighbor-changes

Command	Description
router bgp	Enables the BGP protocol.

Platform Description

None

5.36. bgp maxas-limit

Use this command to set the maximum number of ASs in the BGP AS-PATH attribute. Use the **no**

default form of the command to restore the default configuration.

bgp maxas-limit *number* no bgp maxas-limit default bgp maxas-limit

Parameter Description

Parameter	Description
<i>number</i>	The maximum number of ASs in the BGP AS-PATH attribute. The range is from 1 to 512.

Defaults

No maximum number of ASs is set by default.

Command Mode

BGP configuration mode/ BGP scope global configuration mode.

Usage Guide

The routes exceeding the AS number limit are discarded directly. After changing the configuration, use the **clear** command to reset the neighbor and make the configuration take effect.

Configuration Examples

The following example sets the maximum number of ASs in the BGP AS-PATH attribute to 100.

```
QTECH(config-router)# bgp maxas-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.37. bgp maximum-prefix

Use this command to restrict the maximum number of routes in the BGP global or specified VRF. Use the **no** or **default** form of the command to restore the default configuration.

bgp maximum-prefix *numbers* [**vrf** *vrf-name*] **no bgp maximum-prefix** [**vrf** *vrf-name*]
default bgp maximum-prefix [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
<i>vrf-name</i>	Indicates name of a specific VRF.
<i>numbers</i>	Indicates number of routes. Range: 1 to 4,294,967,295.

Defaults

The function is disabled by default.

Command Mode

BGP configuration mode/ BGP scope global configuration mode.

Usage Guide

When a route advertisement in an address family causes the current number of BGP routes to exceed the maximum number, a prompt indicating route overflow in the global or specified VRF is displayed, and the BGP global or specified VRF is set to the overflow state.

The BGP routing information prefix may be introduced by **redistribute**, from a neighbor or from another VRF. In either case, once the BGP routing information prefix of an address family is introduced, the number of BGP global or specified VRF routes reaches the upper limit, the prefix will not increase and a prompt indicating route overflow in the global or specified VRF is displayed, and the BGP global or specified VRF is set to the overflow state.

Run the **show bgp { addressfamily | all } summary** command to check routing information base status.

If the address family enters the overflow state because the BGP routing information prefix reaches the upper limit, it can be adjusted by **maximum-prefix**.

For IPv4 unicast routes, the routing information prefix may still be received if it is in the overflow state in the following cases:

The routing information of the same routing prefix already exists in the routing information base;

A route that covers the prefix (except the default route) already exists in the routing information base, and the next hop of the route is different from the next hop of the newly received route prefix.

Configuration

The following example sets the maximum number of routes to 100.

Examples

```
QTECH(config)#router bgp 100
QTECH(config-router)#bgp maximum-prefix 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.38. bgp mp-error-handle session-retain

Use this command to retain BGP sessions when BGP protocol detects errors in multi-protocol route attributes. Use the **no** or **default** form of this command to restore the default setting.

bgp mp-error-handle session-retain [refresh-timer *time*]

no bgp mp-error-handle session-retain default bgp mp-error-handle session-retain

Parameter Description

Parameter	Description
-----------	-------------

refresh-timer <i>time</i>	Configures the waiting time for auto route recovery. The parameter ranges from 10 to 4294967296 in the unit of seconds. The default is 120.
----------------------------------	--

Defaults

By default, BGP sessions will be interrupted when multi-protocol attribute errors are detected.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

By default, when UPDATA packets are received from a neighbor, BGP sessions will be interrupted if multi-protocol attribute errors are detected, which will cause oscillation of routes of all the address families of the neighbor. An address family's route error will affect the stability of routes of other address families. After this command is configured, when an error of the route attribute of an address family occurs, all the route information of the address family and neighbor will be deleted, thus preventing impact on the BGP session and other protocol address families, improving BGP protocol's stability.

The option `recovery-time` is used to configure the waiting time for auto route recovery. To use the option, the neighbor must support the route refreshing capability. After recovery-time expires, BGP will send a route-refresh message to the neighbor's address family and re-notify the neighbor of the address family's all route information.

Configuration Examples

The following example retains BGP sessions when BGP protocol detects errors in multi-protocol route attributes.

```
QTECH(config-router)# bgp mp-error-handle session-retain
```

Configuration Examples

Command	Description
N/A	N/A

Platform Description

N/A

5.39. bgp nexthop trigger delay

Use this command to configure the delay time for updating the routing table when the nexthop of the BGP route changes. Use the no or default form of this command to restore the default setting.

bgp nexthop trigger delay *delay-time* no bgp nexthop trigger delay default bgp nexthop trigger delay

Parameter Description

Defaults

The default is 5.

Parameter	Description
<i>delay-time</i>	Delay time for updating the routing table when the nexthop changes, in the range from 0 to 100 in the unit of seconds

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command is used to configure the delay time for updating the routing table when the nexthop changes, it takes effect when the bgp nexthop trigger enable switch is opened.

Configuration Examples

The following example retains BGP sessions when BGP protocol detects errors in multi-protocol route attributes.

```
QTECH(config-router)# bgp nexthop trigger delay 30
```

Related Commands

Command	Description
bgp nexthop trigger enable	Enables the nexthop trigger.

Platform Description

None

5.40. bgp nexthop trigger enable

Use this command to enable the nexthop trigger update function. Use the **no** or **default** form of this command to disable this function.

bgp nexthop trigger enable **no bgp nexthop trigger enable**

default bgp nexthop trigger enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address-family configuration mode, BGP IPv4/IPv6 VRF address-family configuration mode, BGP L2VPN EVPN address family configuration mode, BGP VPNv4/VPNv6 address-family configuration mode or BGP Scope configuration mode.

Usage Guide

This command is used to enable the nexthop trigger update function.

Configuration Examples

Related Commands

The following example enables the nexthop trigger update function.

QTECH(config-router)# **bgp nexthop trigger enable**

Command	Description
Bgp nexthop trigger delay	Sets the delay time for updating the routing table when the nexthop changes.

Platform Description

None

5.41. bgp notify unsupport-capability

Use this command to enable the neighbor address family capability detection function. Use the **no** or

default form of this command to restore the default setting.

bgp notify unsupport-capability

no bgp notify unsupport-capability default bgp notify unsupport-capability

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

When BGP neighbor address family capability negotiation is not fully consistent, neighbors can still be connected. After this command is configured, when an address family capability supported by the local device is not supported by the neighbor device, Notification packet that carries the address family that does not support the capability will be send.

Configuration Examples

The following example enables the neighbor address family capability detection function.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp notify unsupport-capability
```

Configuration Examples

Command	Description
router bgp	Enables BGP protocol.

Platform Description

N/A

5.42. bgp redistribute-internal

Use this command to control BGP whether to allow redistributing routes learned from IBGP, such as RIP, OSPF and ISIS, to the IGP protocol. Use the no or default form of this command to disable this function.

bgp redistribute-internal no bgp redistribute-internal

default bgp redistribute-internal

Parameter Description

Parameter	Description
N/A	N/A

Defaults

IBGP routes are allowed by default to be redistributed to the IGP protocol.

Command Mode

BGP configuration mode, IPv4/IPv6 Unicast address family configuration mode, IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command is used to control whether IBGP routes are allowed to be redistributed to the IGP protocol.

Configuration

The following example enables the BGP to learn the redistributing routes from IBGP.

Examples

```
QTECH(config-router)# bgp redistribute-internal
```

Related Commands

Command	Description
redistribute	Redistributes routes learned from other protocols.

Platform Description

None

5.43. bgp router-id

Use this command to configure the ID-IP address of the device. Use the **no** or **default** form of this command to restore the default setting.

bgp router-id *ip-address* no bgp router-id default bgp router-id

Parameter Description

Parameter	Description
<i>ip address</i>	IP address

Defaults

The loop-back interface of the device is selected preferentially by default. If it does not exist, the device route-id of the device is used.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope Global configuration mode.

Usage Guide

This command is used to configure IP address, the ID of the device when running the BGP protocol.

Configuration Examples

Command	Description
show ip bgp dampening dampened-paths	Displays the suppressed routing information.
bgp dampening	Enables the route dampening function and sets dampening parameters.

Related Commands

The following example configures the ID-IP address of the device.

```
QTECH(config-router)# bgp router-id 10.0.0.1
```

Platform

Description

None

5.44. bgp scan-rib disable

Use this command to update the routing table by event triggering. Use the **no** or **default** form of this command to restore the default setting.

bgp scan-rib disable

no bgp scan-rib disable default bgp scan-rib disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Timely scan and update is enabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address-family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP L2VPN EVPN address family configuration mode and BGP Scope configuration mode.

Usage Guide

BGP provides two route update mechanisms: regular-scanning update and event-triggering update. Regular-scanning update indicates that BGP uses an internal timer to start scanning regularly and update the routing table. Event-triggering update indicates that BGP starts scanning and updates the routing table when the BGP configuration commands are changed due to user configuration or the next hop of a BGP route changes.

Configuration Examples

Related Commands

The following example configures the timely scan for the BGP protocol.

```
QTECH(config-router)# bgp scan-rib disable
```

Command	Description
bgp scan-time	Configures the interval for the BGP timely scan.

Platform Description

None

5.45. bgp scan-time

Use this command to configure the interval for the BGP timely scan. Use the no or default form of this command to restore the default setting.

```
bgp scan-time time no bgp scan-time default bgp scan-time
```

Parameter Description

Parameter	Description
<i>time</i>	Interval of the timely scan, in the range from 5 to 60 in the unit of seconds

Defaults

The default is 60.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, or BGP Scope configuration mode.

Usage Guide

This command is used to configure the interval for the BGP timely scan; it takes effect when `bgp scan-rib enable` is configured.

Configuration Examples

Related Commands

The following example configures the interval for the BGP timely scan.

```
QTECH(config-router)# bgp scan-time 30
```

Command	Description
<code>bgp scan-rib enable</code>	Enables timely scan of the routing table by BGP.

Platform Description

None

5.46. `bgp tcp-source-check disable`

Use this command to configure BGP's TCP source check function. Use **no** or **default** form of this command to disable this function.

```
bgp tcp-source-check disable
```

```
no bgp tcp-source-check disable default bgp tcp-source-check disable
```

Parameter Description

Parameter	Description
-	-

Defaults

This function is enabled by default.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide After TCP source check function is disabled, all TCP connection requests will be received. After TCP connection is established, if no neighbor peer is configured on the local device, Notification packet will be send to refuse the BGP connection.

Configuration Examples

The following example configures BGP's TCP source check function.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp tcp-source-check disable
```

Configuration Examples

Command	Description
router bgp	Enables BGP protocol.

Platform Description

N/A

5.47. bgp timer accuracy-control

Use this command to configure BGP's internal timer accuracy control. Use **no** or **default** form of this command to restore the default setting.

bgp timer accuracy-control no bgp timer accuracy-control

default bgp timer accuracy-control

Parameter Description

Parameter	Description
-	-

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode

Usage Guide

By default, a deviation from the given time will occur on the BGP protocol's timer to prevent concurrent overtime of many timers. You can use this command to configure BGP protocol's

timer to strictly implement the given time. It is recommended disabling this function unless necessary.

Configuration Examples

The following example configures BGP's internal timer accuracy control.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# bgp timer accuracy-control
```

Configuration Examples

Command	Description
router bgp	Enables BGP protocol.

Platform Description

N/A

5.48. bgp update-delay

Use this command to set the maximum delay time of the BGP Speaker before sending the first updating information to neighbors. The no or default form of the command restores it to the default value. During the BGP graceful-restart, this command is used to update the delay time.

bgp update-delay *delay-time* no bgp update-delay default bgp update-delay

Parameter Description

Defaults

The default is 120.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Parameter	Description
<i>delay-time</i>	Maximum delay time of the BGP Speaker before sending its route updating information, in the range from 0 to 3600 in the unit of seconds, 120 seconds by default. For BGP graceful-restart, it is the maximum time of waiting to receive the EOR message of all neighbors, in the range from 1 to 3600 in the

	unit of seconds.
--	------------------

Usage Guide

With the BGP starting up, it first waits some time to connect with its neighbors, and then sends the updating message to these neighbors. After connecting with neighbors, the BGP does not send the updating message to them immediately, but waits some time to receive the updating routing message from all neighbors and then performs routing optimization calculation and finally advertises the route updating message to its neighbors, which improves the convergence time and reduces the calculation consumption. If the software sends the route updating information to its neighbors immediately, it may send the information again when it receives more optimized routes from other neighbors.

The `bgp update-delay` command is used to adjust the initial waiting time of the software, which is the maximum time, from establishing the connection with the first neighbor to performing the routing optimization calculation and sending the route advertisement. When the BGP graceful-restart is enabled, this command is also used to set the maximum waiting time to receive EOR messages from all neighbors. You can increase this value if there are many neighbors or the routing information of the neighbors is huge. If the number of neighbors is 100 and the average amount of routes is 5000, the update sending time that each neighbor completes all the routing is 1 second, then the update of all the routing needs 100 seconds; if the number of neighbors increases to 200, the Update Delay time can be set to 240 seconds, ensuring that all the routing can be updated with the Update Delay period. The specific time is also related to data transmission rate.

Configuration Examples

The following example sets the update-delay time to 200 seconds.

```
QTECH(config)# router bgp 500
QTECH(config-router)# bgp graceful-restart
```

```
QTECH(config-router)# bgp update-delay 200
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform Description

None

5.49. clear bgp all

Use this command to reset all BGP address-families. The content to be reset depends on the further parameters .

clear bgp all [*as number*] [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
<i>none parameter</i>	Resets peer sessions in all address-families.
<i>as-number</i>	Resets sessions with all members in the specified AS. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.
in	Resets the received routing information.
out	Resets the redistributed routing information.
soft	Soft-resets all routing information received/sent from/to the specified peer.
soft in	Soft-resets the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to reset sessions of all supported address-families, including the vrf session in every address-family.

Configuration Examples

N/A

Related Commands

Command	Description
clear bgp ipv4 unicast	Resets the IPv4 unicast address-family.

Platform

None

Description**5.50. clear bgp all peer-group**

Use this command to reset BGP's specific peer group. The reset content is determined by further parameters.

```
clear bgp all peer-group peer-group-name [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
<i>peer-group-name</i>	Resets a specific peer group.
in	Resets received route information.
out	Resets allocated route information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -**Command Mode**

Privileged EXEC mode

Usage Guide

This command will reset replies of all supported address families, including reply connection included in vrf in each address family.

Configuration -

Examples

Configuration Examples

Command	Description
clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.

Platform Description

5.51. clear bgp all update-group

Use this command to reset sessions of all members in an update-group.

clear bgp all update-group [*update-group-index* | *peer-address*] [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of
	members need to be reset.
<i>peer-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.
-	Resets BGP sessions directly if no option is carried.
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets sent and received routing information.
soft in	Soft-resets received routing information.
soft out	Soft-resets distributed routing information.

Command Mode

Privileged EXEC mode

Default Level

14**Usage Guide**

This command is used to reset BGP sessions of all members in an update-group.

Configuration Example

The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1.1.1.1 belongs.

```
QTECH# clear bgp all update-group 1.1.1.1 in
```

5.52. clear bgp ipv4 unicast

Use this command to reset BGP IPv4 unicast address families. The reset content is determined by further parameters.

clear bgp ipv4 unicast [**vrf** *vrf-name*] { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
*	Resets all peer group sessions under address families.
<i>as-number</i>	Resets sessions with all members in the specified AS.
<i>peer-address</i>	Resets sessions with the specified peer.
in	Resets received route information.
out	Resets allocated route information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is the same as **clear ip bgp** in terms of the function and parameters.

Configuration Examples

Configuration Examples

Platform Description

N/A

Command	Description
N/A	N/A

N/A

5.53. clear bgp ipv4 unicast dampening

Use this command to clear the flap information and disable route dampening.

clear bgp ipv4 unicast [vrf *vrf-name*] dampening [*ip-address* [*mask*]]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
-	Clears the flap information of all routes.
<i>address</i>	IP address
<i>mask</i>	Mask

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the BGP route dampening information and release suppressed routes. This command can be used to restart the BGP route dampening.

Configuration Examples

Related Commands

The following example clears the flap information and disables route dampening.

```
QTECH# clear ip bgp dampening 192.168.0.0255.255.0.0
```

Command	Description
show ip bgp dampening dampened-paths	Displays the suppressed routing information.
bgp dampening	Enables the route dampening and sets the dampening parameters.

Platform Description

None

5.54. clear bgp ipv4 unicast external

Use this command to reset all EBGP connections.

```
clear bgp ipv4 unicast [ vrf vrf-name ] external [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
in	Resets received route information.
out	Resets allocated route information.
soft	Soft-resets all routing information received/sent from/to the specified peer.
soft in	Soft-resets the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to reset the specified external BGP connection.

Configuration Examples

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp neighbors	Displays the neighbor information.

Related Commands

The following example resets all EBGp connections.

```
QTECH# clear bgp ipv4 unicast external in
```

Platform Description

None

5.55. clear bgp ipv4 unicast flap-statistics

Use this command to clear the route flap information.

clear bgp ipv4 unicast [**vrf** *vrf-name*] **flap-statistics** [*address* [*mask*]]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
-	Clears all route flap information
<i>address</i>	IP address
<i>mask</i>	Mask

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command can be used only to clear the statistics of unsuppressed routes. It does not release the suppressed routes. To clear all route statistics and release the suppressed routes, run the **clear ip bgp dampening** command.

Configuration Examples

The following example clears the route flap information.

```
QTECH# clear bgp ipv4 unicast flap-statistics
```

Related Commands

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.56. clear bgp ipv4 unicast peer-group

Use this command to reset the session with all members in the peer group.

```
clear bgp ipv4 unicast [ vrf vrf-name ] peer-group peer-group-name [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
<i>peer-group-name</i>	Name of the peer group
in	Resets received route information.
out	Resets allocated route information.
soft	Soft-resets all routing information received/sent from/to the specified peer.
soft in	Soft-resets for the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command resets the BGP session with all members in the peer group.

Configuration Examples

Related Commands

The following example resets the session with all members in the peer group.

```
QTECH# clear bgp ipv4 unicast peer-group my-group in
```

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.57. clear bgp ipv4 unicast table-map

Use this command to update the table-map setting under the IPv4 unicast address family of BGP.

clear bgp ipv4 unicast [vrf *vrf-name*] table-map

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide

Re-apply table-map setting and update allocated core route table information.

Configuration Examples

Parameter Description

Command	Description
clear ip bgp	Resets BGP's IPv4 unicast address families.

Platform Description

5.58. clear bgp ipv4 unicast update-group

Use this command to reset sessions of all members in an update-group in the IPv4 unicast address family.

Parameter Description

Parameter	Description
<i>vrf-name</i>	Specifies the name of a VRF instance. A global VRF instance is used if no VRF instance name is entered.
<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of members need to be reset.
<i>peer-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.
-	Resets BGP sessions directly if no option is carried.
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets sent and received routing information.
soft in	Soft-resets received routing information.

soft out	Soft-resets distributed routing information.
-----------------	--

Command Mode

```
clear bgp ipv4 unicast [ vrf vrf-name ] update-group [ update-group-index | peer-address ]
[ soft ] [ in | out ]
```

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to reset BGP sessions of all members in an update-group in the IPv4 unicast address family.

Configuration Example

The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1.1.1.1 in the IPv4 unicast address family belongs.

```
QTECH# clear bgp ipv4 unicast update-group 1.1.1.1 in
```

5.59. clear bgp ipv6 unicast

Use this command to reset BGP's IPv6 unicast address families.

```
clear bgp ipv6 unicast [ vrf vrf-name ] { * | as-number | peer-address } [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
vrf-name	VRF name
*	Resets all peer group sessions under address families.
as-number	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte

	AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535
	in the dotted mode.
<i>peer-address</i>	Resets sessions with the specified peer.
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide

The function is similar with **clear bgp ipv4 unicast**, but applies to different address families.

Configuration Examples

Configuration Examples

Command	Description
clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.

Platform -

Description

5.60. clear bgp ipv6 unicast dampening

Use this command to clear flap information and disable route dampening.

```
clear bgp ipv6 unicast [ vrf vrf-name ] dampening [ ip-address [ mask ] ]
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
-	Clears all routes' flap information.
<i>ip-address</i>	IP address
<i>mask</i>	Mask code

Command Mode

Privileged EXEC mode

Usage Guide

You can use this command to clear BGP's route flap information and disable route dampening. The command can restart BGP's route flap.

Configuration Examples

Configuration Examples

Platform Description

The following example clears flap information and disables route dampening.

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.

5.61. clear bgp ipv6 unicast external

Use this command to reset all EBGp connection of IPv6 unicast address families.

```
clear bgp ipv6 unicast [ vrf vrf-name ] external [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide

You can use this command to reset all the specified external BGP connection.

Configuration Examples

Configuration Examples

Command	Description
clear ip bgp	Resets BGP sessions.
show ip bgp neighbors	Displays BGP neighbors' information.

The following example resets all EBGp connection of IPv6 unicast address families.

```
QTECH# clear bgp ipv6 unicast external in
```

Platform Description

5.62. clear bgp ipv6 unicast flap-statistics

Use this command to clear IPv6 unicast address families' route flap statistics.

clear bgp ipv6 unicast [*vrf vrf-name*] **flap-statistics** [*address* [*mask*]]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
-	Clears all route information's flap information.
<i>address</i>	IP address
<i>mask</i>	Mask code

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide

This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the **clear bgp ipv4 unicast dampening** command.

Configuration Examples

Configuration Examples

Platform Description

The following example clears IPv6 unicast address families' route flap statistics.

```
QTECH# clear bgp ipv6 unicast flap-statistics
```

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.
show ip bgp	Displays BGP route entries.

5.63. clear bgp ipv6 unicast peer-group

Use this command to reset sessions with all members in the peer group.

clear bgp ipv6 unicast [*vrf vrf-name*] **peer-group** *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
<i>peer-group-name</i>	Peer group name
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to reset BGP sessions with all members in the peer group.

Configuration Examples

Configuration Examples

Platform Description

The following example resets sessions with all members in the peer group.

```
QTECH# clear bgp ipv6 unicast peer-group my-group in
```

Command	Description
clear ip bgp	Resets BGP sessions.
show ip bgp	Displays BGP route entries.

5.64. clear bgp ipv6 unicast table-map

Use this command to update the table-map setting under the IPv6 unicast address family of BGP.

```
clear bgp ipv6 unicast [ vrf vrf-name ] table-map
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide -

Configuration Examples

Configuration Examples

Command	Description
---------	-------------

clear ip bgp	Resets BGP's IPv4 unicast address families.
---------------------	---

Platform Description

5.65. clear bgp ipv6 unicast update-group

Use this command to reset sessions of all members in an update-group in the IPv6 unicast address family.

clear bgp ipv6 unicast [**vrf** *vrf-name*] **update-group** [*update-group-index* | *neighbor-address*] [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
vrf-name	Specifies the name of a VRF instance. A global VRF instance is used if no VRF instance name is entered.
update-group-index	Specifies the index of an update-group, in which the sessions of members need to be reset.
neighbor-address	Specifies the update-group, to which a peer whose session needs to be reset belongs.
-	Resets BGP sessions directly if no option is carried.
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets sent and received routing information.
soft in	Soft-resets received routing information.
soft out	Soft-resets distributed routing information.

Command Mode

Privileged EXEC mode

Default Level **14**

Usage Guide

This command is used to reset BGP sessions of all members in an update-group in the IPv6 unicast address family.

Configuration Example

The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1111::1111 in the IPv6 unicast address family belongs.

```
QTECH# clear bgp ipv6 unicast update-group 1111::1111 in
```

5.66. clear bgp l2vpn evpn

Use this command to reset BGP EVPN address families.

```
clear bgp l2vpn evpn { * | as-number | neighbor-address } [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
*	Resets all peer group sessions under address families.
<i>as-number</i>	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.
<i>neighbor-address</i>	Resets sessions with the specified peer.
in	Resets received route information.
out	Resets allocated route information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide The function is similar with `clear bgp ipv4 unicast`, but applies to different address families.

Configuration Examples

Configuration Examples

Command	Description
clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.

Platform Description

5.67. clear bgp l2vpn evpn dampening

Use this command to clear flap information and disable route dampening.

`clear bgp l2vpn evpn dampening`

Parameter Description

Parameter	Description
N/A	

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide

You can use this command to clear BGP's route flap information and relieve damped routes. The command can restart BGP's route flap.

Configuration Examples

The following example clears flap information and disables route dampening.

```
QTECH# clear bgp l2vpn evpn dampening
```

Platform Description

N/A

5.68. clear bgp l2vpn evpn external

Use this command to reset all EBGp connection of BGP EVPN address families.

clear bgp l2vpn evpn external [soft] [in | out]

Parameter Description

Parameter	Description
in	Resets received route information.
out	Resets allocated route information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

You can use this command to reset all the specified external BGP connection.

Configuration Examples

The following example resets all EBGp connection of L2VPN EVPN address families.

```
QTECH# clear bgp l2vpn evpn external in
```

Platform Description

N/A

5.69. clear bgp l2vpn evpn flap-statistics

Use this command to clear BGP EVPN address families' route flap statistics.

clear bgp l2vpn evpn flap-statistics

Parameter Description

Parameter	Description
N/A	

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the **clear bgp l2vpn evpn dampening** command.

Configuration Examples

The following example clears L2VPN EVPN address families' route flap statistics.

```
QTECH# clear bgp l2vpn evpn flap-statistics
```

Platform Description

N/A

5.70. clear bgp l2vpn evpn peer-group

Use this command to reset sessions of all members in the peer group.

```
clear bgp l2vpn evpn peer-group peer-group-name [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
<i>peer-group-name</i>	Peer group name
in	Resets received route information.
out	Resets allocated route information.
soft	Soft-resets received and sent route information.

soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to reset BGP sessions of all members in the peer group.

Configuration Examples

The following example displays that the L2VPN EVPN address family soft-resets received route information of all members in the peer group my-group.

```
QTECH# clear bgp l2vpn evpn peer-group my-group in
```

Platform Description

N/A

5.71. clear bgp l2vpn evpn update-group

Use this command to reset sessions of all members in an update-group of L2VPN EVPN address family.

clear bgp l2vpn evpn update-group [*update-group-index* | *peer-address*] [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of members need to be reset.
<i>peer-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.

-	Resets BGP sessions directly if no option is carried.
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets sent and received routing information.
soft in	Soft-resets received routing information.
soft out	Soft-resets distributed routing information.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to reset BGP sessions of all members in an update-group of L2VPN EVPN address family.

Configuration Example

The following example resets routing information received by all peers in an update group of L2VPN EVPN address family to which the peer with the IP address of 1.1.1.1 belongs.

```
QTECH# clear bgp l2vpn evpn update-group 1.1.1.1 in
```

5.72. clear evpn conflict mac

Use this command to clear MAC information and other statistics of conflicts occurring in EVPN.

Parameter Description**Command Mode**

clear evpn conflict mac [*vni-id*]

Parameter	Description
	Clears MAC information and other statistics of conflicts occurring on a

<i>vni-id</i>	specified L2VNI.
---------------	------------------

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to clear conflict MAC information and re-advertise the EVPN routes corresponding to the conflict MAC.

Configuration Example

The following example clears all conflict MAC information.

```
QTECH# clear evpn conflict mac
```

5.73. clear ip bgp

Use this command to reset the BGP session.

clear ip bgp [vrf *vrf-name*] { * | *as-number* / *peer-address* } [soft] [in | out]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
*	Resets all the current BGP sessions and the OVERFLOW status of BGP ipv4 unicast address family.
<i>address</i>	Resets the BGP session with the specified peer.
<i>as number</i>	Resets sessions with all members in the specified AS. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.

in	Reset the received routing information.
out	Reset the distributed routing information.
soft	Soft-reset all routing information received/sent from/to the specified peer
soft in	Soft-reset the received routing information.
soft out	Soft-reset the distributed routing information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

At any time, once the routing policy or BGP configuration changes, an effective way must be available to implement the new routing policy or configuration. Traditional measure is to close the BGP connection and establish a new one.

This product supports implementing a new routing strategy without closing the BGP session connection by soft-resetting BGP.

For the peer that does not support the route refresh function, you may run the **neighbor soft-reconfiguration inbound** command to keep a copy of original routing information of every specified BGP peer on the local BGP speaker. This will consume some resources.

You can use the **show ip bgp neighbors** command to see whether the BGP peer supports the route refresh function. If it is supported, you need not to execute the **neighbor soft-reconfiguration inbound** command when the inbound routing strategy changes.

All connected BGP routers must support the route refresh function to execute this command.

This product supports the route refresh function.

Configuration Examples

Related Commands

The following example resets the BGP session.

```
QTECH# clear bgp ipv4 unicast *
```

Command	Description
---------	-------------

neighbor soft-reconfiguration inbound	(Optional) Restarts the BGP session and reserves the unchanged route information sent by the BGP peer (group).
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.74. clear ip bgp dampening

Use this command to clear the dampening information and disable route dampening.

clear ip bgp [vrf *vrf-name*] dampening [*ip-address* [*mask*]]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
<i>address</i>	IP address
<i>mask</i>	Mask

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the BGP route flap information and disable route dampening. This command can be used to restart BGP route dampening.

Configuration Examples

Related Commands

The following example clears the dampening information and disables route dampening.

QTECH# clear ip bgp dampening 192.168.0.0 255.255.0.0

Command	Description
---------	-------------

show ip bgp dampening dampened-paths	Displays the suppressed routing information.
bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform Description

None

5.75. clear ip bgp external

Use this command to reset all EBGp connections.

`clear ip bgp [vrf vrf-name] external [soft] [in | out]`

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
in	Reset the received routing information.
out	Reset the distributed routing information.
soft in	Soft-resets the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to reset the specified external BGP connection.

Configuration Examples

Related Commands

The following example resets all EBGp connections.

`QTECH# clear ip bgp external in`

Platform Description

None

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp neighbors	Displays the neighbor information.

5.76. clear ip bgp flap-statistics

Use this command to clear the routes vibration statistics of the IPv4 unicast address family.

clear ip bgp [vrf *vrf-name*] flap-statistics [*ip-address* [*mask*]]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
<i>address</i>	IP address
<i>Mask</i>	Mask

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command can be used only to clear statistics of unsuppressed routes. It does not release the suppressed routes. To clear all route statistics and release the suppressed routes, run the **clear ip bgp dampening** command.

Configuration Examples

Related Commands

The following example clears the routes vibration statistics of the IPv4 unicast address family.

```
QTECH# clear ip bgp flap-statistics
```

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.77. clear ip bgp peer-group

Use this command to reset the session with all members in the peer group.

```
clear ip bgp [ vrf vrf-name ] peer-group peer-group-name [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
<i>peer-group-name</i>	Name of the peer group
in	Reset the received routing information.
out	Reset the distributed routing information.
soft	Soft-resets all routing information received/sent from/to the specified peer
soft in	Soft-resets the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command resets the BGP session with all members in the peer group.

Configuration Examples

Related Commands

The following example resets the session with all members in the peer group.

```
QTECH# clear ip bgp peer-group my-group in
```

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.78. clear ip bgp table-map

Use this command to update the table-map's route information applied by IPv4 unicast address family.

clear ip bgp [vrf *vrf-name*] table-map

Parameter Description

Parameter	Description
<i>vrf-name</i>	vrf name

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to update the route information of the applied table-map.

Configuration Examples

The following example updates the table-map's route information applied by IPv4 unicast address family.

```
QTECH# clear ip bgp table-map
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.79. clear ip bgp update-group

Use this command to reset sessions of all members in an update-group in the IPv4 unicast address family.

```
clear ip bgp [ vrf vrf-name ] update-group [ update-group-index | neighbor-address ]
[ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	Specifies the name of a VRF instance. A global VRF instance is used if no VRF instance name is entered.
<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of members need to be reset.
<i>neighbor-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.
-	Resets BGP sessions directly if no option is carried.
in	Resets received routing information.
out	Resets distributed routing information.
soft	Soft-resets sent and received routing information.
soft in	Soft-resets received routing information.
soft out	Soft-resets distributed routing information.

Command Mode

Privileged EXEC mode

Default Level 14**Usage Guide**

This command is used to reset BGP sessions of all members in an update-group in the IPv4 unicast address family.

Configuration Example

The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1.1.1.1 in the IPv4 unicast address family belongs.

```
QTECH# clear ip bgp update-group 1.1.1.1 in
```

5.80. default-information originate

Use this command to enable BGP to distribute the default route. Use the **no** form of this command to restore the default setting.

default-information originate [no] default-information originate

default default-information originate

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, BGP IPv4 VRF configuration mode, BGP IPv6 VRF configuration mode

Usage Guide

This command is used to control whether the redistributed default route is effective, and this command needs to be configured together with the **redistribute** command. It takes effect only when a default route exists in the redistributed route.

This command is similar to the **network** command. The difference is that in the process of configuring the former, the **redistribute** command must be configured explicitly to redistribute the default route, only in this case, the redistributed default route is effective. For the later command, the IGP must have the default route.

Configuration Examples

Related Commands

The following example enables BGP to distribute the default route.

```
QTECH(config-router)# default-information originate
```

Command	Description
network	Configures routes to be advertised.
redistribute	Redistributes routes of other protocol.

Platform Description

None

5.81. default-metric

Use this command to set the metric for route redistribution. Use the **no** or **default** form of this command to restore the default setting.

default-metric *number* no default-metric default default-metric

Parameter Description

Parameter	Description
<i>number</i>	Metric number, in the range from 1 to 4294967295

Defaults

No metric is set by default.

Command Mode

BGP configuration mode, BGP IPv4/ IPv6 Unicast address family configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode or BGP Scope configuration mode.

This command sets the metric of routes to be redistributed for integrity.

Usage The metric set by the command cannot cover that set by the **redistribute metric** command.

Guide

The value is 0 when the default metric applies to redistributed connected routes.

Configuration Examples

Related Commands

The following example sets the metric for route redistribution.

```
QTECH(config-router)# default-metric 45
```

Command	Description
redistribute	Redistributes routes of other protocol.

Platform Description

None

5.82. distance bgp

Use this command to set different management distances for different types of BGP routes. Use the **no**

or **default** form of this command to restore the default setting. **distance bgp external-distance internal-distance local-distance no distance bgp**

default distance bgp

Parameter	Description
<i>external-distance</i>	Route management distance learned from EBGp peers, in the range from 1 to 255
<i>internal-distance</i>	Route management distance learned from IBGP peers, in the range from 1 to 255
<i>local-distance</i>	Specifies the management distance of route learned from peers. However, the optimal one can be learned from the IGP. In general, these routes are indicated by the Network Backdoor command. The value is in the range from 1 to 255

Parameter Description

Defaults

The parameter defaults are as follows:

external-distance - 20

internal-distance - 200

local-distance – 200

Command Mode

BGP configuration mode or BGP Scope configuration mode.

Usage Guide

It is not recommended to change the management distance of the BGP route. If it is necessary, observe the following points:

- The management distance of "external-distance" must be shorter than those of other IGP routing protocols (such as OSPF and RIP);
- The internal-distance and local-distance should have longer management distances than other IGP routing protocols.

Configuration Examples

Related Commands

The following example sets different management distances for different types of BGP routes.

```
QTECH(config-router)# distance bgp 20 20 200
```

Command	Description
neighbor soft-reconfiguration inbound	Restarts the BGP session and reserves the unchanged route information sent by the BGP peer (group).
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.83. evpn

Use this command to enter EVPN configuration mode. Use the no or restore form of this command to restore the default settings.

evpn

no evpn default evpn

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the EVPN configuration mode is disabled.

Command

Mode Global configuration mode

Usage Guide

Use this command to enter EVPN configuration mode. Use the exit command to exit the EVPN configuration mode

Configuration Examples

The following example enters EVPN configuration mode.

```
QTECH(config)# evpn
```

Platform

Description

N/A

3.3 exit-address-family

Use this command to exit BGP address-family configuration mode.

exit-address-family

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

BGP address-family configuration mode

Usage Guide

This command can be used to exit from various address-family modes of BGP to BGP configuration mode.

Configuration Examples

Related Commands

The following example exits the BGP address-family configuration mode.

```
QTECH(config-router-af)#exit-address-family
```

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode.

Platform Description None

5.84. export map(EVPN VNI)

Use this command to configure the route map for exporting the extended community attribute of EVPN routes from the local device to the remote device. Use the no form of this command to delete the route map for exporting the extended community attribute of EVPN routes from the local device to the remote device. Use the default form of this command to restore the default settings.

export map *route-map-name*

no export map default export map

Parameter Description

Parameter	Description
<i>route-map-name</i>	Name of the route map

Defaults

No route map is configured for exporting the extended community attribute by default.

Command Mode

EVPN VNI configuration mode.

Default Level

14

Usage Guide This command is used to modify the extended community attribute advertised by a type 5 route converted from a local EVPN route or IP route.

This command supports only one route map, and the old configuration is overwritten by the new configuration.

Configuration Examples

The following example configures a route map for exporting the extended community attribute associated with map1 on VNI 1.

```
QTECH(config)# evpn QTECH(config-evpn)# vni 1
QTECH(config-evpn-vni)# export map map1
```

Verification

Run the show running-config command to display the configurations.

5.85. import map(EVPN VNI)

Use this command to configure the route map for importing the remote EVPN routes to the local VNI instance. Use the **no** form of this command to delete the route map for importing the remote EVPN routes to the local VNI instance. Use the **default** form of this command to restore the default settings. **import map** *routemap-name*

no import map default import map

Parameter Description

Parameter	Description
<i>routemap-name</i>	Name of the route map

Defaults

No route map is configured for importing the remote EVPN routes to the local VNI instance by default.

Command Mode

EVPN VNI configuration mode.

Default Level

14

Usage Guide

This command is used to filter the remote EVPN routes to be imported to the local VNI instance, or modify the attribute of the remote EVPN routes imported to the local VNI instance.

This command supports only one route map, and the old configuration is overwritten by the new configuration.

Configuration Examples

```
QTECH(config)# evpn QTECH(config-evpn)# vni 1
QTECH(config-evpn-vni)# import map map1
```

The following example configures the route map map1 for importing the remote EVPN routes to the local VNI instance vni 1.

Verification

Run the **show running-config** command to display the configurations.

5.86. maximum-paths

Use this command to configure the number of equivalent paths of the EBGp/IBGP multipath load balancing function. Use the no form of this command to disable the EBGp/IBGP multipath load balancing function. Use the default form of this command to restore the default settings.

maximum-paths { ebgp | ibgp } number **no maximum-paths { ebgp | ibgp } default**
maximum-paths { ebgp | ibgp }

Parameter Description

Parameter	Description
ebgp	Specifies the number of equivalent paths of the EBGp multipath load balancing function.
ibgp	Specifies the number of equivalent paths of the IBGP multipath load balancing function.
number	Indicates the maximum number of equivalent paths. The minimum value is 1, and the maximum value depends on the device capability. If the value is 1, the EBGp multipath load balancing function is disabled.

Defaults

Equivalence of multiple BGP paths is not supported by default.

Command Mode

BGP configuration mode, BGP IPv4 Unicast address family configuration mode, BGP IPv6 Unicast address family configuration mode, and BGP Scope Global configuration mode

Default Level

14

Usage Guide

The maximum-paths ebgp command is also used to configure equivalence of confederation EBGp multiple paths and local inter-VRF import routes.

IBGP and EBGp routes cannot form equivalent routes.

Configuration Examples

The following example configures EBGp load balancing and sets the maximum number of equivalent routes to 2.

```
QTECH(config)# router bgp 65530
QTECH(config-router)# maximum-paths ebgp 2
```

Verification

Run the show running-config command to display the BGP configurations.

5.87. maximum-prefix

Use this command to limit the maximum number of prefixes in the routing database in the address family. Use the **no** or **default** form of this command to restore the default setting.

maximum-prefix *maximum* no maximum-prefix default maximum-prefix

Parameter Description**Defaults**

The maximum number is not limited by default.

Parameter	Description
<i>maximum</i>	The maximum number of prefixes in the routing database in the address family, in the range from 1 to 4294967295

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.

In a BGP address family, routing prefixes may be introduced through redistribution or learnt from neighbors, or other VRFs. Once routing prefixes in the BGP address family reaches the maximum number, this address family will enter to the overflow state.

Use the **show bgp** { *addressfamily* | **all** } **summary** command to display the state of routing database.

It is necessary to reconfigure BGP for state clearing, or use the **clear bgp** { *addressfamily* | **all** } * command to reset the address family.

Usage Guide

When the address family is overflow as the number of prefixes reaches the maximum number, you can adjust maximum-prefix.

Maximum-prefix will not filter the routing information generated by the network and aggregate commands.

IPv4 unicast routes can receive the routing prefix in the following conditions even in the Overflow state:

The route information of the same routing prefix exists in the address database.

One route that overwrites this prefix (except for the default route) exists in the address database and the next-hop of this route is different from that of the newly received routing prefix.

Configuration Examples

The following example sets the maximum number of prefixes in the BGP routing database in the ipv4 multicast address family.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# address-family ipv4 multicast QTECH(config-router-af)# maximum-
prefix 65535
```

Related Commands

Command	Description
clear bgp all	Resets BGP's all address families.
clear bgp ipv4 mdt	Resets BGP's ipv4 mdt address families.
clear bgp ipv4 unicast	Resets BGP's ipv4 unicast address families.
clear bgp ipv6 unicast	Resets BGP's ipv6 unicast address families.
clear bgp vpnv4 unicast	Resets BGP's vpnv4 unicast address families.
show bgp all summary	Displays summary of BGP's all address families.
show bgp ipv4 mdt summary	Displays summary of BGP's ipv4 mdt address

	families.
show bgp ipv4 unicast summary	Displays summary of BGP's ipv4 unicast address families.
show bgp ipv6 unicast summary	Displays summary of BGP's ipv6 unicast address families.
show bgp vpnv4 summary	Displays summary of BGP's vpnv4 unicast address families.

Platform Description

N/A

5.88. neighbor activate

Use this command to activate the neighbor or peer group in the current address mode. Use the **no** or

default form of this command to disable this function. **neighbor {peer-address | peer-group-name} activate no neighbor {peer-address | peer-group-name} activate**

default neighbor { peer-address | peer-group-name } activate

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 address or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Parameter Description

Defaults

This function is enabled in IPv4 address family mode by default.

Command Mode

BGP configuration mode, BGP IPv4/ IPv6 Unicast address family configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration

mode, or BGP Scope configuration mode.

Usage Guide

The function is enabled by default for IPv4 address families. You need to set this command in other address-family configuration modes for exchanging routes.

The following example activates the neighbor or peer group in the current address mode.

Configuration Examples

```
QTECH(config)# router bgp 60
QTECH(config-router)# neighbor 10.0.0.1 remote-as 100 QTECH(config-router)# address-
family vpnv4 QTECH(config-router-af)# neighbor 10.0.0.1 activate
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.89. neighbor advertisement-interval

Use this command to set the time interval to send the BGP route update message. Use the **no** or

default form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **advertisement-interval** *seconds* **no**
neighbor { *peer-address* | *peer-group-name* } **advertisement-interval** **default** **neighbor**
 { *peer-address* | *peer-group-name* } **advertisement-interval**

Parameter Description

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>seconds</i>	Time interval to send the route update message in the range from 0 to 600 seconds

Defaults

IBGP connection: 15 seconds EBGP connection: 30 seconds

Command Mode

BGP configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command.

Configuration The following example sets the time interval to send the BGP route update message.

Examples

```
QTECH(config)# router bgp 60
QTECH(config-router)# neighbor 10.0.0.1 remote-as 100
QTECH(config-router)# neighbor 10.0.0.1 advertisement-interval 10
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.90. neighbor allowas-in

Use this command to allow the PE to receive messages with the same AS number as itself. Use the **no**

or **default** form of this command to restore the default setting. **neighbor** {*peer-address* | *peer-group-name*} **allowas-in** *number* **no neighbor** {*peer-address* | *peer-group-name*} **allowas-in default neighbor** {*peer-address* | *peer-group-name*} **allowas-in**

Parameter Description

Defaults

This function is disabled by default.

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32

	characters
<i>number</i>	Number of the AS number duplication in the range from 1 to 10, 3 by default

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

A typical application is spoke_hub mode. Execute this command on the PE to enable it to receive and then send the advertised address prefix. Configure two VRFs on the PE. One VRF receives the routes of all PEs and advertises them to the CE; the other VRF receives the routes advertised by the CE and advertises them to all PEs.

This command applies to IBGP or EBGP peers.

The following example allows the PE to receive messages with the same AS number as itself.

Configuration Examples

```
QTECH(config)# router bgp 60
QTECH(config-router)# neighbor 10.1.1.1 remote-as 100 QTECH(config-router)# address-family ipv4 vrf vpn1
QTECH(config-router-af)# neighbor 10.1.1.1 allowas-in
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.91. neighbor as-originate-interval

Use this command to configure the interval that the device advertises local original BGP routes to the peer (group). Use the **no** or **default** form of this command to restore the default setting.

neighbor { peer-address | peer-group-name } as-origination-interval seconds no neighbor { peer-address | peer-group-name } as-origination-interval default neighbor { peer-address | peer-group-name } as-origination-interval

Parameter Description

Parameter	Description
<i>peer address</i>	IP address of the peer.
<i>peer-group-name</i>	Name of the peer group, containing up to 32 characters.
<i>seconds</i>	The interval at which the device advertises local original BGP routes to the peer (group), in the range from 1 to 65535 in the unit of seconds.

Defaults

The default interval is 1.

Command Mode

BGP configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP IPv6 VRF address family configuration mode/ BGP scope global configuration mode.

Usage Guide

If you specify a peer group name in this command, the configuration takes effect on all members of the peer group.

Configuration Examples

The following example configures the interval at which the device advertises local original BGP routes to the peer in the BGP IPv4 VRF address family configuration mode.

```
QTECH(config)# router bgp 60
QTECH(config-router)# address-family ipv4 vrf vpn1 QTECH(config-router-af)# neighbor
10.0.0.1 remote-as 100
QTECH(config-router-af)# neighbor 10.0.0.1 as-origination-interval 10
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

5.92. neighbor default-originate

Use this command to allow the BGP speaker to advertise the default route to the peer (group). Use the

no or default form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} default-originate [*route-map map-tag*] no
neighbor {*peer-address* | *peer-group-name*} default-originate [*route-map map-tag*]

default neighbor { *peer-address* | *peer-group-name* } default-originate [*route-map map-tag*]

Parameter Description

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>map-tag</i>	Name of the route-map of up to 32 characters

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, or BGP Scope configuration mode

Usage Guide

This command does not requires the default route but sends a default route whose next-hop address is the local address to neighbors.

If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command. If you set the command for a member in the peer, this command will overwrite the settings on the peer group.

Configuration Examples

The following example allows the BGP speaker to advertise the default route to the peer (group).

```
QTECH(config)# router bgp 60
QTECH(config-router)# neighbor 10.1.1.1 remote-as 80 QTECH(config-router)# neighbor
10.1.1.1 default-originate
```

Related Commands

Command	Description
---------	-------------

router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.93. neighbor description

Use this command to set a descriptive sentence for the specified peer (group). Use the **no** or **default**

form of this command to restore the default setting.

Parameter Description

neighbor {*peer-address* | *peer-group-name*} **description** *text*

no neighbor {*peer-address* | *peer-group-name*} **description** **default** **neighbor** { *peer-address* | *peer-group-name* } **description**

Defaults

This function is disabled by default.

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>text</i>	Descriptive text of the peer (group) of up to 80 characters

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode and BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command is used to add descriptive characters for the peer (group). This may help remember features and characteristics of the peer (group).

Configuration Examples

The following example sets a descriptive sentence for the specified peer (group).

```
QTECH(config)# router bgp 60
QTECH(config-router)# neighbor 10.1.1.1 remote-as 80
QTECH(config-router)# neighbor 10.1.1.1 description xyz.com
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform**Description** None**5.94. neighbor distribute-list**

Use this command to implement the routing policy based on the ACL when receiving/sending route information from/to the specified BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **distribute-list** { *access-list-number* } { **in** | **out** }

no neighbor { *peer-address* | *peer-group-name* } **distribute-list** { *access-list-number* } { **in** | **out** }

default neighbor { *peer-address* | *peer-group-name* } **distribute-list** { *access-list-number* | *access-list-name* } { **in** | **out** }

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>access-list-number</i>	ACL number
in	Specifies the ACL for filtering the incoming routes.
out	Specifies the ACL for filtering the outgoing routes.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage Guide

For in rule or out rule, this command cannot be used together with the **neighbor prefix-list** command. Only one of them can take effect.

If you have specified the BGP peer group, all members of the peer group will adopt the settings. If you set the **neighbor distribute-list** command for a member in the peer, this command will overwrite the settings on the peer group.

You can set different filtering policies in different address-family configuration modes to control routes.

Configuration Examples

The following example implements the routing policy based on the ACL when receiving/sending route information from/to the specified BGP peer.

```
QTECH(config)# router bgp 60
QTECH(config-router)# neighbor 10.1.1.1 remote-as 80
QTECH(config-router)# neighbor 10.1.1.1 distribute-list bgp-filter in
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip access-list	Creates a standard IP ACL or extended IP ACL.

Platform

Description None

5.95. neighbor ebgp-multihop

Use this command to allow establishing BGP connection between EBGP peers that are not directly connected. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*tth*]

no neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*tth*]

default neighbor { *peer-address* | *peer-group-name* } **ebgp-multihop** [*tth*]

Parameter	Description
<i>peer address</i>	IP address of the peer

<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>ttl</i>	Maximum hops in the range 1 to 255

Defaults

The BGP connection is allowed between EBGp peers connected with each other directly by default.

If "ebgp-multihop" is followed by no parameter, the ttl is 255.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

To prevent routing loop and dampening, non-default routes that can reach the peer must exist between EBGp peers between which the BGP connection can only be established via multiple hops.

If the BGP peer group is specified, all members of the peer group adopt the settings. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

```
The following example allows establishing BGP connection between EBGp peers that are not
directly connected.QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 remote-as 65100 QTECH(config-router)# neighbor
10.0.0.1 ebgp-multihop
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.96. neighbor fall-over bfd

Use this command to enable BFD correlation with BGP. Use the **no** form or **default** form of this command to disable BFD correlation with BGP.

neighbor { *peer-address* | *peer-group-name* } **fall-over bfd** **no neighbor** { *peer-address* | *peer-group-name* } **fall-over bfd**

default neighbor { *peer-address* | *peer-group-name* } **fall-over bfd**

Parameter Description

Parameter	Description
<i>peer address</i>	IPv4 or IPv6 address of the peer.
<i>peer-group-name</i>	Name of the peer group, containing up to 32 characters.

Defaults

BFD correlation is disabled by default.

Mode configuration mode/ Scope configuration mode

Usage Guide

Before configuring BFD correlation, the BFD session parameters of the neighbor interface must be configured.

Configuration Examples

The following example enables BFD correlation to detect the forwarding path between local and the neighbor 172.16.0.2.

```
QTECH(config)# router bgp 45000
QTECH(config-router)# neighbor 172.16.0.2 remote-as 45001 QTECH(config-router)# neighbor
172.16.0.2 fall-over bfd
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.97. neighbor filter-list

Use this command to enable route filtering when sending/receiving routing information to/from BGP peers. Use the no or default form of this command to restore the default setting.


```
neighbor { peer-address | peer-group-name } filter-list access-list-number { in | out }
```

```
no neighbor { peer-address | peer-group-name } filter-list access-list-number { in | out }
```

```
default neighbor { peer-address | peer-group-name } filter-list access-list-number { in | out }
```

Parameter Description

Parameter	Description
<i>peer address</i>	IP address of the peer, IPv4 address or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>access-list-number</i>	ACL number
in	Applies as-path list on the received routing information.
out	Applies as-path list on the distributed routing information.

Defaults

The function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage Guide

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If the **neighbor filter-list** command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example enables route filtering when sending/receiving routing information to/from BGP peers.

```
QTECH(config)# ip as-path access-list 1 deny _123_ QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 remote-as 65100
QTECH(config-router)# neighbor 10.0.0.1 filter-list 1 out
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip as-path access-list	Creates an AS_PATH list.
match as-path	Matches the AS_PATH list.

Platform Description

None

5.98. neighbor local-as

Use this command to configure the local AS number for the BGP peer, which could be used as its Remote AS to connect with local router. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} local-as *as-number* [no-prepend [replace-as [dual-as]]]

no neighbor {*peer-address* | *peer-group-name*} local-as default neighbor { *peer-address* | *peer-group-name* } local-as

Parameter	Description
<i>peer address</i>	IP address of the peer, IPv4 address or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>as-number</i>	Local AS number, in the range from 1 to 65535. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.
no-prepend	The AS-PATH of the routing information received from the peer does not depend on the Local AS. This option is disabled by default.
replace-as	The AS-PATH of the routing information sent to the peer replaces the BGP AS with the Local AS. This option is disabled by default.

dual-as	Uses BGP AS or Local AS to establish BGP connection with the device. This option is disabled by default.
----------------	--

Parameter Description

Defaults

No Local AS is configured for the peer. If Local AS is configured, no option is configured by default. The peer could only use Local AS to establish BGP connection with local device, and adds Local AS into the AS-PATH of the received routing information, inserts Local AS to the corresponding

AS-PATH before sending the routing information to the peer.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 VRF configuration mode or BGP Scope configuration mode.

Usage Guide

Local AS could be configured on the EBGP peer only, and if the attributes of the peer change, such as EBGP converts to IBGP or union EBGP, Local AS and corresponding options will be deleted.

Local AS must be different from BGP AS and this peer's Remote AS and the union ID (if federation is configured). If you have specified the BGP peer group, all members of this peer group will adopt the settings of this command. You cannot set Local AS for the specified member of the peer group separately.

Configuration Examples

The following example configures the local AS number for the BGP peer.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 remote-as 65100
QTECH(config-router)# neighbor 10.0.0.1 local-as 23
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

N/A

5.99. neighbor maximum-prefix

Use this command to limit the number of prefixes received from the specified BGP peer. Use the no or

default form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} maximum-prefix *maximum* [*threshold*] [warning-only]

no neighbor {*peer-address* | *peer-group-name*} maximum-prefix *maximum*

default neighbor { *peer-address* | *peer-group-name* } maximum-prefix *maximum*

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>maximum</i>	Upper limit of the number of the received route entries
<i>threshold</i>	Percentage of the maximum when alarming.
warning-only	Does not terminate the BGP connection when the route entries reach the upper limit but produce a log entry.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

The BGP connection will be torn down when the received routes exceeds the upper limit by default. To prevent tearing down the connection, set the "warning-only" to control that.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example limits the number of prefixes received from the specified BGP peer.

```
QTECH(config)# router bgp 65000
```

```
QTECH(config-router)# neighbor 10.0.0.1 maximum-prefix 1000
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.100. neighbor next-hop-self

Use this command to set the next-hop of the route to the local BGP speaker while specifying the routes that the BGP peer redistributes. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **next-hop-self** **no neighbor** {*peer-address* | *peer-group-name*} **next-hop-self**

default neighbor { *peer-address* | *peer-group-name* } **next-hop-self**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage

This command is mostly used in the non-full-mesh-type network, such as the Frame Relay and

Guide

X.25, where the BGP speakers within the same subnet cannot completely be accessed mutually. If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command.

Configuration Examples

The following example sets the next-hop of the route to the local BGP speaker.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 next-hop-self
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.101. neighbor next-hop-unchanged

Use this command to maintain the next-hop when sending routes to the peer(group). Use the no or

default form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} next-hop-unchanged no neighbor {*peer-address* | *peer-group-name*} next-hop-unchanged

default neighbor { *peer-address* | *peer-group-name* } next-hop-unchanged

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
next-hop-unchanged	Maintains the next-hop while sending the routes to the peer(group).

Defaults

The next-hop will be changed by default when routes are sent to the EBGp peer.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope Global configuration mode.

Usage Guide

This command is used to control to maintain the next-hop route transmitting between multi-hop EBGP peer sessions. This command cannot be configured on the route reflector. And for the client of the route reflector, if this function is enabled, the neighbor next-hop-self command cannot be used to change the next-hop of routes. This function is mainly applied to the cross-domain VPN. In the implementation with the Option C adopted, to reduce the complete connectivity between the PEs of the cross-domain CPN, a route reflector can be set in every autonomous domain to establish the Multihop MP-EBGP connection to implement the VPN route interaction. As the

next-hop route is changed as itself while sending routes to the EBGP peer by default, PE stations of other autonomous domains will consider the final next-hop of the VPN route as the route reflector

when receiving the VPN route at last, which will result in all cross-domains VPN flow going through the reflector. However, usually this is not the optimal forwarding path, and the requirement for the forwarding performance of the RR is higher. To avoid this condition, use the neighbor

next-hop-unchanged command in the address-family VPNv4 configuration mode to maintain the next-hop of the VPNv4 route sent to the BGP peer when establishing the cross-domain Multihop MP-EBGP connection on the router reflector.

The following example maintains the next-hop when sending routes to the peer (group).

Configuration Examples

```
QTECH(config)# router bgp 60 QTECH(config-router)# address-family vpnv4
QTECH(config-router-af)# neighbor 10.1.1.1 next-hop-unchanged
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.102. neighbor password

When the BGP connection with the BGP peer is established, use this command to enable TCP MD5 authentication and set the password. Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} **password** [0 | 7]string

no neighbor {*peer-address* | *peer-group-name*} **password default neighbor** { *peer-address* | *peer-group-name* } **password**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
0	Displays the password with encryption.
7	Displays the password without encryption.
<i>string</i>	Password for MD5 authentication in the range from up to 80 characters

Defaults

The function is disabled by default

Command Mode

BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command will enable MD5 authentication of the TCP. BGP peers must have the same password configured; otherwise, the neighbor relationship cannot be established. When this

command is set, the local BGP speaker will re-establish the BGP connection with the BGP peer.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

No matter in which mode, a neighbor has only one password, not one for every address family, .

Configuration Examples

The following example enables TCP MD5 authentication and sets the password.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 password Red-Giant
```


Command	Description
router bgp	Enables the BGP protocol
neighbor remote-as	Configures the BGP peer.

Platform

Description

None

5.103. neighbor peer-group (creating)

Use this command to create a BGP peer group. Use the **no** or **default** form of this command to restore the default setting.

neighbor *peer-group-name* **peer-group** **no neighbor** *peer-group-name* **peer-group**
default neighbor *peer-group-name* **peer-group**

Parameter Description

Parameter	Description
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults

No BGP peer group is created.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 VRF configuration mode or BGP Scope configuration mode.

Usage Guide

If multiple BGP peers use the same update policy, the peers can be configured in the same peer group, so as to simplify the configuration and boost operation efficiency.

Configuration Examples

The following example creates a BGP peer group.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor Red-Giant peer-group
```


Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
neighbor peer-group (assigning members)	Configures the specified peer as the member of the BGP peer group.
show ip bgp peer-group	Displays the information of the BGP peer.

Platform Description

None

5.104. neighbor peer-group (assigning members)

Use this command to configure the specified peer as a member of the BGP peer group. Use the **no** or

default form of this command to restore the default setting.

neighbor *peer-address* **peer-group** *peer-group-name*

no neighbor *peer-address* **peer-group** *peer-group-name*

default neighbor *peer-address* **peer-group** *peer-group-name*

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults

No peer exists in the peer group.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

Members of the peer group can adopt all configurations of the peer.

It is allowed to configure an individual member of the peer group to replace the universal configuration for the peer group, but such separate configuration does not contain the configuration information that may affect the output update. In other words, every member in the peer group will always adopt the following configurations of the peer group:

remote-as, update-source, local-as, reconnect-interval, times, advertisement-interval, default-originate, next-hop-self, remove-private-as, send-community, distribute-list out, filter-list out, prefix-list out, route-map out, unsuppress-map, route-reflector-client.

Do not place neighbors of different address families in the same peer group, or place IBGP and EBGP neighbors in the same peer group.

The following example configures the specified peer as a member of the BGP peer group.

Configuration Examples

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor Red-Giant peer-group
QTECH(config-router)# neighbor 10.0.0.1 peer-group Red-Giant
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
neighbor peer-group (creating)	Creates the BGP peer group.
show ip bgp peer-group	Displays the information of the BGP peer.

Platform Description

None

5.105. neighbor prefix-list

Use this command to implement the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **prefix-list** *prefix-list-name* { **in** | **out** }

no neighbor {*peer-address* | *peer-group-name*} **prefix-list** *prefix-list-name* { **in** | **out** }

default neighbor { *peer-address* | *peer-group-name* } **prefix-list** *prefix-list-name* { **in** | **out** }

Parameter Description

Parameter	Description
<i>peer address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>prefix-lis-name</i>	Name of the prefix-list of up to 32 characters
in	Applies the prefix list to the received routes.
out	Applies the prefix list to the redistributed routes.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage Guide

For the "in" rule or "out" rule, this command cannot be used together with the **neighbor distribute-list** command. That is, only one of them takes effect.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If the **neighbor prefix-list in** command is set for a member of the peer, the setting will overwrite the setting for the group.

You can set different filter policies in different address-family configuration modes to control routes.

Configuration Examples

The following example implements the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer.

```
QTECH(config)# ip prefix-list bgp-filter deny 10.0.0.1/16
```

```
QTECH(config)# router bgp 65000
```

```
QTECH(config-router)# neighbor 10.0.0.1 prefix-list bgp-filter in
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip prefix-list	Creates the prefix lists.

Platform Description

None

5.106. neighbor remote-as

Use this command to configure the BGP peer (group). Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **remote-as** *as-number*

no neighbor { *peer-address* | *peer-group-name* } **remote-as** **default** **neighbor** { *peer-address* | *peer-group-name* } **remote-as**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>as-number</i>	BGP peer (group) autonomous system number in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.

Defaults

No BGP peer is configured.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Configuration Examples

The following example configures the BGP peer (group).

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 remote-as 80
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

Platform Description

None

5.107. neighbor remove-private-as

Use this command to delete the private AS number recorded in the AS path attribute in the route sent to the specified EBGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **remove-private-as** **no neighbor** {*peer-address* | *peer-group-name*} **remove-private-as**

default neighbor { *peer-address* | *peer-group-name* } **remove-private-as**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32

	characters
--	------------

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, or BGP IPv4 VRF configuration mode.

Usage Guide

This command takes effect only on EBGp peers.

If the AS path contains the private AS number that is the AS number of the EBGp peer to be sent, the AS number is not deleted.

Private AS number range: 64512 - 65535

Configuration Examples

The following example deletes the private AS number recorded in the AS path attribute in the route sent to the specified EBGp peer

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 remove-private-as
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.108. neighbor route-map

Use this command to enable route match for the received/sent routes. Use the no or default form of this command to disable this function.

`neighbor { peer-address | peer-group-name } route-map map-tag {in | out}`

`no neighbor { peer-address | peer-group-name } route-map map-tag {in | out} default`

`neighbor { peer-address | peer-group-name } route-map map-tag { in | out }`

Parameter Description

Parameter	Description
-----------	-------------

<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>map-tag</i>	Name of the match rule
in	Applies the rule to the incoming routes.
out	Applies the rule to the outgoing routes.

Defaults

N/A

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command can be used to filter the incoming and outgoing routes for different neighbors by using different incoming/outgoing rules, purifying and controlling routes.

You can set different filter policies in different address-family configuration modes to control routes.

Configuration Examples

Related Commands

The following example enables route match for the received/sent routes.

```
QTECH(config-router)# neighbor 10.0.0.1 route-map map-tag in
```

Command	Description
neighbor soft-reconfiguration inbound	Stores the routing information sent from the BGP peer.
show ip bgp	Displays the BGP route entry.

Platform Description

None

5.109. neighbor route-reflector-client

Use this command to configure the local device as the route reflector and specifies its client. Use the

no or **default** form of this command to restore the default setting.

neighbor *peer-address* **route-reflector-client** **no neighbor** *peer-address* **route-reflector-client**

default neighbor { *peer-address* | *peer-group-name* } **route-reflector-client**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer. The name cannot exceed 32 characters.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

By default, all IBGP speakers in the autonomous system must establish neighbor relationship with each other. The BGP speaker does not forward the routes learned from an IBGP peer to other IBGP peers to avoid route loop.

This command can be used to set route reflector, so that there is no need for all IBGP speakers to establish full neighboring relationship between each other. This will allow the route reflector to forward learned IBGP routes to other IBGP peers.

Configuration Examples

The following example configures the local device as the route reflector and specifies its client.

```
QTECH(config)# router bgp 65000
```



```
QTECH(config-router)# neighbor 10.0.0.1 route-reflector-client
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
bgp cluster-id	Configures the cluster ID of the route reflectors.
bgp client-to-client reflection	Enables the route reflection between clients

Platform Description

None

5.110. neighbor send-community

Use this command to transmit community attributes to the specified BGP neighbor. Use the no or

default form of this command to restore the default setting.

```
neighbor {peer-address | peer-group-name} send-community [both | standard | extended]
no neighbor {peer-address | peer-group-name} send-community [both | standard |
extended] default neighbor { peer-address | peer-group-name } send-community [ both |
standard |
extended ]
```

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
both	Transmits both standard and extended communities.
standard	Transmits the standard community only.
extended	Transmits the extended community only.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4 Unicast VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode, BGP scope configuration mode

Usage Guide

This command transmits the community to the neighbor or neighbor group.

Configuration Examples**Related Commands**

The following example transmits community attributes to the specified BGP neighbor.

```
QTECH(config-router)# neighbor 10.1.1.1 send-communityboth
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip community-list	Creates the community list.

Platform Description

None

5.111. neighbor shutdown

Use this command to disconnect the BGP connection established with the specified BGP peer. Use the

no or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **shutdown**

no neighbor {*peer-address* | *peer-group-name*} **shutdown** **default neighbor** { *peer-address* | *peer-group-name* } **shutdown**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address

<i>peer-group-name</i>	Name of the peer group of up to 32 characters
------------------------	---

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command is used to disconnect valid connection established with the specified peer (group), and delete all associated routing information. However, this command still keeps the configuration information of that specified peer (group).

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example disconnects the BGP connection established with the specified BGP peer.

```
QTECH(config)# router bgp 60
QTECH(config-router)# neighbor 10.0.0.1 shutdown
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
show ip bgp summary	Displays the BGP connection status.

Platform Description

None

5.112. neighbor soft-reconfiguration inbound

Use this command to store the routing information sent from the BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **soft-reconfiguration inbound** **no neighbor** {*peer-address* | *peer-group-name*} **soft-reconfiguration inbound**

default neighbor { *peer-address* | *peer-group-name* } **soft-reconfiguration inbound**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4 Unicast VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP scope configuration mode

Usage Guide

This command restarts the BGP session, and keeps the unchanged routing information sent from the BGP peer (group).

Executing this command will consume more memories. If both parties support the route refresh function, this command becomes unnecessary. You may run the **show ip bgp neighbors** command to judge whether the peer can support the route refresh function.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example stores the routing information sent from the BGP peer.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 soft-reconfiguration inbound
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

show ip bgp neighbors	Displays the information of the BGP peer.
clear ip bgp	Resets the BGP peer session.

Platform Description

None

5.113. neighbor timers

In specifying BGP peer to establish the BGP connection, use this command to set the keepalive and holdtime time values used for establishing the BGP connection. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **timers** *keepalive* *holdtime* [*minimum-holdtime*] | **connect**

connect-retry }

no neighbor [*peer-address* | *peer-group-name*] **timers** [**connect**]

default neighbor { *peer-address* | *peer-group-name* } **timers** [**connect**]

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>keepalive</i>	Time interval to send the KEEPALIVE message to the BGP peer. Range: 0-65535 seconds
<i>holdtime</i>	Time interval to consider the BGP peer alive Range: 0-65535 seconds
<i>minimum-holdtime</i>	Allows a minimum holdtime value of neighbor advertisement. It is unrestricted when the value is 0. The range is 0 to 65535 seconds.
<i>connect-retry</i>	The value of the connect-retry timer is 15s.

Defaults

keepalive: 60 seconds

holdtime: 180 seconds

minimum-holdtime: 0 seconds

connect-retry: 15 seconds

Command Mode

BGP configuration mode, BGP IPv4 VRF address family configuration mode, BGP IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

A proper keepalive value must not exceed one-third of the holdtime value.

If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example sets the keepalive and holdtime time values used for establishing the BGP connection.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 80 240
```

The following example sets the connect-retry time values used for establishing the BGP connection.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 timers connect 100
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
timers bgp	Sets the keepalive and holdtime values globally.

Platform Description

None

5.114. neighbor unsuppress-map

Use this command to selectively advertise routing information suppressed by aggregate-address command. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **unsuppress-map** *map-tag*

no neighbor {*peer-address* | *peer-group-name*} **unsuppress-map** *map-tag*

default neighbor { *peer-address* | *peer-group-name* } **unsuppress-map** *map-tag*

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>map-tag</i>	Name of the route-map of up to 32 characters

Defaults This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4 Unicast/VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode BGP VPNv4/VPNv6 address family configuration mode, BGP scope configuration mode

Usage Guide

This command advertises the specified suppressed routes.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example selectively advertises routing information suppressed by aggregate-address command.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 unsuppress-map unspress-route
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
aggregate-address	Configures the aggregate address.
route-map	Configures the route-map

Platform Description

None

5.115. neighbor update-delay

Use this command to configure the time of BGP delayed advertisement for first routes. Use the **no** or

restore form of the command to restore the default setting. **neighbor** { *peer-address* | *peer-group-name* } **update-delay** *time* **no neighbor** { *peer-address* | *peer-group-name* } **update-delay default neighbor** { *peer-address* | *peer-group-name* } **update-delay**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>time</i>	Time of BGP delayed advertisement for first routes.

Defaults

The function is disabled by default.

Command

BGP configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP IPv6 VRF

Usage Guide

After BGP starts, BGP peers negotiate to establish the neighborhood before sending route information (update packets).

In addition, after **update-delay** is configured on the local end, a specific neighbor sends route information to the local end, the local end will send out the route information after the delay time. If the BGP peer group is specified, all members of the peer group adopt the settings of this command.

Configuration Examples

The following example sets the delayed time to 60s.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 update-delay 60
```

Platform Description

N/A

3.4 neighbor update-source

Use this command to configure the interface for BGP connection of the IBGP peer..

neighbor { *peer-address* | *peer-group-name* } **update-source** {interface-type interface-number | address }

Use the **no** form of the command to remove the source address configuration for the BGP peer.

no neighbor {*peer-address* | *peer-group-name*} **update-source**

Use the **default** form of the command to restore the default settings.

default neighbor { *peer-address* | *peer-group-name* } **update-source**

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>interface-type</i> <i>interface-number</i>	Interface name
<i>address</i>	The interface address which is used for BGP connection. The address type (IPv4 or IPv6) must be same as that of the peer address.

Parameter Description

Defaults

The local interface is used as the egress interface by default.

Command Mode

BGP configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode/ Scope configuration mode

Guidepeer.

The interface address specified for BGP connection must be valid in local, otherwise the BGP connection may be faulty.

All members in a BGP peer group inherit the settings of this command. Particularly, if the interface address is used, only the member whose address type is same as the interface address's can inherit the settings of this command.

If the IPv6 address of the loopback interface is used for neighbor connection, both peers need to be configured with the loopback interface. The BGP connection can be established only when the address of the egress interface on the peer is same as that of the neighbor in local.

A loopback interface address can be configured on different interfaces. You need to specify only the interface name,

The peer configured with the IPv6 address of loopback interface support only one-hop BGP neighbor connection.

Configuration Examples

The following example establishes the BGP connection.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# neighbor 10.0.0.1 update-source loopback 1
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.116. neighbor version

Use this command to display the number of the BGP protocol version used by the specific BGP neighbor. Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **version** 4

no neighbor { *peer-address* | *peer-group-name* } **version default** **neighbor** { *peer-address* | *peer-group-name* } **version**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32

	characters
4	Version number

Defaults

The default version number is 4.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode

Usage Guide

When the command is used, BGP will lose the version negotiation function.

Configuration Examples

Related Commands

The following example displays the number of the BGP protocol version used by the specific BGP neighbor.

```
QTECH(config-router)# neighbor 10.1.1.1 version 4
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

PlatformDescription

None

5.117. neighbor weight

Use this command to set the weight for the specific neighbor. Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **weight** *number* **no neighbor** { *peer-address* | *peer-group-name* } **weight default neighbor** { *peer-address* | *peer-group-name* } **weight**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32

	characters
<i>number</i>	Weight, in the range from 0 to 65535.

Defaults

No weight is configured for the specific neighbor by default. In this case, the learned route weight is 0 and the locally generated route's weight is 32768 initially.

Command Mode

BGP configuration mode, BGP IPv4 Unicast/VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP scope configuration mode and BGP L2VPN EVPN family address configuration mode

Usage Guide

When the command is used, routes learnt from the neighbor use this value as the initial weight value. The higher the weight, the higher the priority is.

Executing the **set weight** command in the route map of the neighbor will overwrite this value.

Configuration Examples

Related

The following example sets the weight for the specific neighbor.

```
QTECH(config-router)# neighbor 10.1.1.1 weight 73
```

Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.118. network

Use this command to configure the network information to be advertised by the local BGP speaker. Use the no or default form of this command to restore the default setting.

```

network network-number [mask mask] [route-map map-tag] [backdoor]
no network network-number [mask mask] [route-map map-tag] [backdoor]
default network network-number [ mask mask ] [ route-map map-tag ] [ backdoor ]

```

Parameter Description

Parameter	Description
<i>network-number</i>	Network number
<i>mask</i>	Subnet mask
<i>map-tag</i>	Name of the route-map of up to 32 characters
backdoor	The route is a backdoor route.

Defaults

No network information is specified by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command allows injecting the IGP route into the BGP routing table. The network information advertised can be direct route, static route and dynamic route.

The "route-map" can be used to modify the network information.

Configuration Examples

The following example configures the network information to be advertised by the local BGP speaker.

```

QTECH(config)# router bgp 65000
QTECH(config-router)# network 10.0.0.1 mask 255.255.0.0

```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
redistribute	Configures the route redistribution.
Network synchronization	Enables network synchronization.

Platform Description

5.119. network synchronization

Use this command to advertise the network information after the local BGP speaker is synchronized with the local device. Use the **no** or **default** form of this command to directly advertise the network information.

network synchronization no network synchronization

default network synchronization

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

This command is used to modify the status of the network during the process of advertisement. It is not recommended to turn off this switch lest route black hole is caused.

Configuration Examples

The following example advertises the network information after the local BGP speaker is synchronized with the local device.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# network synchronization
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
redistribute	Configures the route redistribution.
network(BGP)	Configures the route to be distributed.

Platform Description

None

5.120. overflow memory-lack

Use this command to allow BGP to enter the OVERFLOW state when the memory is insufficient. Use the no or default form of this command to disable this function.

overflow memory-lack

no overflow memory-lack default overflow memory-lack

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Allow the BGP to enter the OVERFLOW state when the memory is insufficient.

Command Mode

BGP configuration mode or BGP Scope Global configuration mode

Usage Guide

In the BGP OVERFLOW state, the newly-learned routes are discarded, which prevents the memory from increasing.

When this function is enabled, if the BGP address family is in the OVERFLOW state, the newly-learned routes will be discarded, which may result in network loop. To prevent this, BGP

generates a default route directing to the NULL interface, and the default route will always exist in the OVERFLOW state.

Use the clear bgp {addressfamily|all} * command to reset the BGP and clear the OVERFLOW state in the BGP address family.

Use the no option to disallow the BGP to enter the OVERFLOW state when the memory is insufficient, which may lead to the continuous exhaustion of the memory resources. When the memory has been exhausted to a certain degree, BGP will break down all neighbors and delete all learned routes.

Configuration Examples

The following example sets BGP not to enter the OVERFLOW configuration status when the memory is insufficient.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# no overflow memory-lack
```

Related Commands

Command	Description
<code>clear bgp { <i>addressfamily</i> all } *</code>	Resets the BGP address family.
<code>show bgp { <i>addressfamily</i> all } summary</code>	Displays the summary of the BGP address family.

Platform Description

None

5.121. rd

Use this command to configure a RD value for the EVI instance. Use the **no** or **restore** form of this command to restore the default settings.

rd { **auto** | *rd_value* }

no rd { **auto** | *rd_value* } **default rd**

Parameter Description

Parameter	Description
auto	Generates the RD value automatically.
<i>rd_value</i>	<p>Indicates value of the RD. There are 3 forms of <i>rd_value</i>:</p> <ol style="list-style-type: none"> <i>rd_value</i> = <i>as_num</i>:<i>nn</i> The <i>as_num</i> indicates the public AS number (2 bytes) and <i>nn</i> is customized. The range is from 0 to 4,294,967,295. <i>rd_value</i> = <i>ip_addr</i>:<i>nn</i> The <i>ip_addr</i> refers to the global IP address and <i>nn</i> is customized. The range is from 0 to 65,535. <i>rd_value</i> = <i>as4_num</i>:<i>nn</i> The <i>as4_num</i> indicates the public AS number (2

bytes) and nn is customized. The range is from 0 to 65,535.

The 4-byte AS notation range is from 1 to 4,294,967,295, represented as from 1 to 65535.65535 in dot mode.

Defaults

The RD value is not configured by default.

Command Mode

evpn-vni configuration mode

If an EVI is configured with a RD value, the RD value cannot be revised. If you want to revise it, you can only delete the EVI first and then configure a new RD value for it. One EVI can be configured with one RD value only.

Usage Guide

The RD format in 4-byte AS is **AS4:NN**. The **AS4** supports demical and dot mode. The range of **AS4** is from 1 to 4,294,967,295, represented as from 1 to 65535.65535 in dot mode. The

range of **NN** is from 1 to 65,535.

For AS number in the range of 1 to 65,535, it will be saved in the format of 2-byte AS, because under this condition, the demical and dot mode AS are the same.

The following example sets RD for EVI 100. The value is 100 : 1.

```
QTECH(config)# evpn QTECH(config-evpn)# vni
100
QTECH(config-evpn-vni)# rd 100:1
```

Configuration Examples

The following example sets RD for EVI 200. The value is auto.

```
QTECH(config)# evpn
QTECH(config-evpn)# vni 200 QTECH(config-evpn-
vni)# rd auto
```

Platform Description

N/A

5.122. redistribute

Use this to redistribute routes between the other routing protocol and the BGP. Use the **no** or **default**

form of this command to restore the default setting.

redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

no redistribute *protocol-type* [**route-map** *map-tag*] [**metric**]

default redistribute protocol-type [**route-map** *map-tag*] [**metric**]

Parameter	Description
<i>protocol-type</i>	The source protocol types for redistributing routes, including connected, static, RIP
route-map <i>map-tag</i>	Specifies the route map. No route map is associated with by default.
metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by default.

Parameter Description

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol. This is applicable to all IP routing protocols.

Usage Guide

When you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The no form removes redistribution without any parameters configured.

The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are unavailable, the redistributed one is used.

Configuration Examples

The following example redistributes routes between the other routing protocol and the BGP.

```
QTECH(config-router)# redistribute static route-map static-rmap
```

Related Commands

Command	Description
show ip protocol	Displays the protocol configuration.

Platform Description

None

5.123. redistribute ospf

Use this command to redistribute routes between OSPF and BGP. Use the **no** or **default** form of this command to restore the default setting.

redistribute ospf *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [1|2]]

nssa-external [1|2]]

no redistribute ospf *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external**

[1|2] *nssa-external* [1|2]]

default redistribute ospf *process-id* [**route-map** *map-tag*] [**metric**] [**match { internal | external** [1

| 2] | *nssa-external* [1 | 2] }]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID to be redistributed
route-map <i>map-tag</i>	Specifies the route map. No route map is associated by default.
metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by

	default.
match	Matches the sub type of OSPF routes.
internal	Matches the internal OSPF routes, the default configuration.
external [1 2]	Matches the external OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.
nssa- external [1 2]	Matches the NSSA-external type of OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol.

Usage Guide

When you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.

The filtering rule of OSPF routing: filtering the OSPF routing type according to the configured match option before filtering the route-map rule. The route metric generated by the **route-map**

command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Configuration Examples

The following example redistributes routes between OSPF and BGP.

```
QTECH(config-router)# redistribute ospf 2 route-map static-rmap
```

Related Commands

Command	Description
show ip protocol	Displays the protocol configuration.

Platform Description

None

5.124. redistribute isis

Use this command to redistribute routes between ISIS and BGP. Use the no or default form of this command to restore the default settings.

`redistribute isis [isis-tag] [route-map map-tag] [metric metric-value] [level-1 | level-1-2 | level-2]`
`no redistribute isis [isis-tag] [route-map map-tag] [metric] [level-1 | level-1-2 | level-2]`

`default redistribute isis [isis-tag] [route-map map-tag] [metric] [level-1 | level-1-2 | level-2]`

Parameter	Description
<i>isis-tag</i>	(Optional)ISIS process ID to be redistributed
route-map <i>map-tag</i>	Specifies the route map. No route map is associated by default.
metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by default.
level-1	Redistributes level-1 ISIS routes.
level-1-2	Redistributes level-1 and level-2 ISIS routes.
level-2	Redistributes level-2 ISIS routes.

Parameter Description**Defaults**

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol. This is applicable to all IP routing protocols.

When you configure the no form of this command with parameters, the corresponding parameter configuration will be removed. The no form removes redistribution without any parameters configured.

The filtering rule of ISIS routing is: filtering the ISIS routing type according to the configured level option before filtering the route-map rule. The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are unavailable, the redistributed one is used.

Configuration Examples

Related Commands

The following example redistributes routes between ISIS and BGP.

```
QTECH(config-router)# redistribute isis route-map static-rmap
```

Command	Description
show ip protocol	Displays the protocol configuration.

Platform Description

None

5.125. route-target

Use this command to configure a RT (Route Target) for EVI. Use the **no** or **restore** form of this command to restore the default settings.

route-target { **import** | **export** | **both** } { **auto** | *rt_value* }

no route-target { **import** | **export** | **both** } { **auto** | *rt_value* }

default route-target { **import** | **export** | **both** } { **auto** | *rt_value* }

Parameter Description

Parameter	Description
auto	Generates the RD value automatically.
import	Sets the import RT value.

export	Sets the export RT value.
both	Sets the import and export RT value.
<i>rt_value</i>	<p>Indicates value of the RT. There are 3 forms of <i>rt_value</i>:</p> <p><i>rt_value</i> = <i>as_num</i>:<i>nn</i></p> <p>The <i>as_num</i> indicates the public AS number (2 bytes) and <i>nn</i> is customized. The range is from 0 to 4,294,967,295.</p> <p><i>rt_value</i> = <i>ip_addr</i>:<i>nn</i></p> <p>The <i>ip_addr</i> refers to the global IP address and <i>nn</i> is customized. The range is from 0 to 65,535.</p> <p><i>rt_value</i> = <i>as4_num</i>:<i>nn</i></p> <p>The <i>as4_num</i> indicates the public AS number (2 bytes) and <i>nn</i> is customized. The range is from 0 to 65,535.</p> <p>The 4-byte AS notation range is from 1 to 4,294,967,295, represented as from 1 to 65535.65535 in dot mode.</p>

Defaults

The RT value is not configured by default.

Command Mode

evpn-vni configuration mode

Guide

The format of auto RT is **AS2:NN**. The **AS2** is the AS number of 2B. If an AS number of 4B is configured, it will be split into two 2B AS number and then be put in the RT. The **nn** indicates

value of **vni-id** and has a space of 4B.

If the AS number of BGP changes, the auto RT will be changed, too.

If the manually configured RT is coherent with the auto RT, both will be displayed. After the **auto** command is configured and the automatically generated RT value is 100 : 1, then if you delete value 100 : 1, only the value not the **auto** command will be deleted.

The following example sets RT for EVI 100. The values are import RT 100:1, 100:4, export RT 100:2, 100:4, and both auto.

Configuration Examples

```
QTECH(config)# evpn QTECH(config-evpn)# vni
100
QTECH(config-evpn-vni)# route-target import 100:1 QTECH(config-evpn-
vni)# route-target export 100:2 QTECH(config-evpn-vni)# route-target
both 100:4
QTECH(config-evpn-vni)# route-target both auto
```

Platform Description

N/A

3.5 router bgp

Use this command to enable the BGP protocol, configure the local autonomous system number and enter BGP protocol configuration mode. Use the no or default form of this command to restore the default setting.

`router bgp as-number`

`no router bgp as-number`

`default router bgp as-number`

Parameter Description

Parameter	Description
<i>as-number</i>	AS number in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Guide RFC4839 defines a new reserved AS notation 23456, which cannot be used. The original private AS notation in the range from 64512 to 65534 is still effective, 65535 is reserved for special purposes.

RFC 5398 also defines two groups of new reserved AS notation for documents, whose ranges are from 64496 to 64511 and from 65536 to 65551.

Configuration Examples

Related Commands

The following example enables the BGP protocol.

```
QTECH(config)# router bgp 65000
```

Command	Description
ip routing	Enables IP routing.
bgp router-id	Sets the ID of the device running the BGP protocol
network	Sets the network information to be advertised by the local BGP speaker.

Platform Description

None

5.126. synchronization

Use this command to enable the synchronization mechanism of BGP and IGP routing information. Use the **no** or **default** form of this command to restore the default settings.

synchronization

no synchronization default synchronization

Parameter Description

Defaults

This function is disabled by default.

Parameter	Description
N/A	N/A

Command Mode

```
QTECH(config)# router bgp 65000
```

```
QTECH(config-router)# table-map bgp_tm
```

VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

The synchronization between BGP and IGP aims to prevent the possible route black hole.

In any of the two cases below, you may cancel the synchronization mechanism to ensure fast convergence of routing information.

There is no route information which passes through this AS (In general, this AS is an end AS).

All devices within this AS operate BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).

```
QTECH(config)# router bgp 65000
QTECH(config-router)# table-map bgp_tm
```

Examples information.

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

Platform Description

None

5.127. table-map

Use this command to control the route information distributed to the kernel table. Use the no or default

form of this command to restore the default setting.

table-map route-map-name

no table-map default table-map

Parameter Description

Parameter	Description
<i>route-map-name</i>	Name of the route-map

Defaults

No table-map is configured by default,

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# table-map bgp_tm
```

Usage Guide

BGP uses the table-map to control the information distributed to the kernel routing table. The table-map is used to modify attributes of that route information, and it only takes effect on the IPv4 address-family.

Configuration Examples

The following example controls the route information distributed to the kernel table.

Related Commands

Command	Description
route-map	Configures the route-map

Platform Description

None

5.128. timers bgp

Use this command to adjust the BGP network timer. Use the no or default form of this command to restore the default value.

`timers bgp keepalive holdtime [minimum-holdtime]`

`no timers bgp default timers bgp`

Parameter Description

Parameter	Description
<i>keepalive</i>	Time interval to send the keepalive message to the BGP peer Range: 0-65535 seconds.
<i>holdtime</i>	Time interval to consider the BGP peer alive Range: 0-65535 seconds.
<i>Minimum-holdtime</i>	Allows a minimum holdtime value of neighbor advertisement. It is unrestricted when the value is 0. The range is 0 to 65535 seconds.

Defaults

keepalive: 60 seconds

holdtime: 180 seconds

minum-holdtime: 0 seconds

Command Mode

BGP configuration mode / BGP scope global configuration mode

Usage Guide

A proper keepalive value must not exceed one-third of the holdtime value.

If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example adjusts the BGP network timer.

```
QTECH(config)# router bgp 65000
QTECH(config-router)# timers bgp 80 240
```

Related Commands

Command	Description
neighbor timers	Sets the keepalive and holdtime values on the basis of neighbors.

Platform Description

None

5.129. how bgp all

Use this command to display all the address-families information of BGP route. The use of this command is consistent with other BGP's show commands.

Display the parameters of the route information.

show bgp all [**community** [*community-number* [**exact-match**]] | **filter-list** *path-list-number* | **community-list** *community-name* [**extact-match**] | **extcommunity-list** *extcommunity-name* | **regex** *regex* | **quote-regex** *regex* | **inconsistent-as**]

Display the route dampening parameter.

show bgp all dampening { flap-statistics | dampened-paths | parameters } Display the related information of the neighbors.

show bgp all neighbors [peer-address [received-routes | routes | advertised-routes | policy [detail]]]

5.130. show bgp all summary

Display the update-group information.

show bgp [instance as-num] all update-group [neighbor-address | update-group-index] [summary]

Parameter Description

Parameter	Description
community community-number	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
community-list community-name	Displays the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matching the community value or community-list.
dampening dampened-paths	Displays the restrained routing information.
dampening flap-statistics	Displays the routing dampening statistics.
dampening parameters	Displays the routing dampening parameters.

extcommunity-list extcommunity-name	Displays the routing information including the specified extcommunity value.
filter-list path-list-number	Displays the routing information matching the filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.
neighbors [peer-address]	Displays all the BGP neighbors' information.
neighbors peer-address received-routes	Displays all routing information received from the specified peer (including the accepted and refused route).
neighbors peer-address routes	Displays all the accepted routing information received from the peer.
neighbors peer-address advertised-routes	Displays all the routing information sent to the specified peer.
neighbors peer-address policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors peer-address policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
quote-regexp regexp	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp regexp	Displays the BGP routing information with the AS path attribute matching the specified regexp.

Summary	Displays BGP neighbor information.
update-group [<i>neighbor-address</i> <i>update-group-index</i>]	Display update-group information. When <i>neighbor-address</i> is specified, display the update-group information of the specified neighbor. When <i>update-group-index</i> is specified, display the specified update-group information.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

The following example shows all neighbors' information.

Configuration Examples

```
QTECH(config)# show bgp all For address family: IPv4

Unicast

BGP table version is 1, local router ID is 1.2.3.4

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*> 1.0.0.0 0.0.0.0 0 32768 ?

Total number of prefixes 1

For address family: IPv6 Unicast
```

BGP table version is 1, local router ID is 1.2.3.4

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path

*> 5750:1::/120 :: 0 32768 ?

Total number of prefixes 1

Related Commands

Command	Description
show bgp ipv4 unicast	Displays the IPv4 unicast route information of BGP

Platform Description

None

5.131. show bgp ipv4 unicast

Use this command to display the IPv4 unicast route information of BGP.

```
show bgp ipv4 unicast [ vrf vrf-name ] [ network [ network-mask [ longer-prefixes ] ] ]
show bgp ipv4 unicast [ vrf vrf-name ] community community-number [ exact-match ]
show bgp ipv4 unicast [ vrf vrf-name ] community-list community-name [ exact-match ]
show bgp ipv4 unicast [ vrf vrf-name ] extcommunity-list extcommunity-name
```

5.132. show bgp ipv4 unicast [vrf vrf-name] dampening dampened-paths

Parameter Description

```
show bgp ipv4 unicast [ vrf vrf-name ] dampening flap-statistics show bgp ipv4
unicast [ vrf vrf-name ] filter-list path-list-number show bgp ipv4 unicast [ vrf vrf-
name ] inconsistent-as
```

```
show bgp ipv4 unicast [ vrf vrf-name ] prefix-list ip-prefix-list-name
```


show bgp ipv4 unicast [vrf *vrf-name*] quote-regexp *regexp*

show bgp ipv4 unicast [vrf *vrf-name*] regexp *regexp*

show bgp ipv4 unicast[vrf *vrf-name*] route-map *map-tag*

show bgp ipv4 unicast [vrf *vrf-name*] neighbors [*neighbor-address* [received-routes | routes | advertised-routes | policy [detail]]]

show bgp ipv4 unicast [vrf *vrf-name*] cidr-only

Parameter	Description
vrf-name	VRF name
network	Displays the specific routing information in the routing table
network-mask	Displays the routing information included in the specified network.
longer-prefixes	Displays the route map information.
community community-number	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
community-list community-name	Displays the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matching the community value or community-list.
extcommunity-list extcommunity-name	Displays the routing information including the specified extcommunity value.
dampening dampened-paths	Displays the restrained routing information.
dampening flap- statistics	Displays the routing dampening statistics.
filter-list path-list-	Displays the routing information matching the

number	filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.
prefix-list ip-prefix-list-name	Displays the routing information matching the specified prefix-list.
quote-regexp regexp	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp regexp	Displays the BGP routing information with the AS path attribute matching the specified regexp.
route-map map-tag	Displays the routing information matching the specified route-map filtering condition.
neighbors	Displays the BGP IPv4 unicast neighbor information.
[<i>neighbor-address</i>]	
neighbors <i>neighbor-address</i> received-routes	Displays all routing information received from the specified peer (including the accepted and refused route).
neighbors <i>neighbor-address</i> routes	Displays all the routing information received from the peer and accepted.
neighbors <i>neighbor-address</i> advertised-routes	Displays all the routing information sent to the specified peer.
neighbors <i>neighbor-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>neighbor-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
cidr-only	Displays the routing information without the category.

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to view the IPv4 unicast route information of BGP. You can filter the information with the specified parameter to display the matching route information.

The following example displays the IPv4 unicast route information of BGP.

Configuration Examples

```
QTECH# show bgp ipv4 unicast
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete Network      Next
Hop      Metric LocPrf Path
*>i44.0.0.0 192.168.195.183 0 100 i
*>i64.12.0.0/16 192.168.195.183 0 100 i
*>i172.16.0.0/24 192.168.195.183 0 100 i
*>i 202.201.0.0 192.168.195.183 0 100 i
*>i 202.201.1.0 192.168.195.183 0 100 i
*>i 202.201.2.0 192.168.195.183 0 100 i
*>i 202.201.3.0 192.168.195.183 0 100 i
*>i202.201.18.0 192.168.195.183 0 100 i
```

```
*>i202.201.0 192.168.195.183 0 100 i
.0
*>i202.201.1 192.168.195.183 0 100 i
.0
*>i202.201.2 192.168.195.183 0 100 i
.0
*>i202.201.3 192.168.195.183 0 100 i
.0
```

5. BGP4 Commands

```
Total number of prefixes 4
QTECH(config)# ip as-path access-list 5 permit .* QTECH# show bgp
ipv4 unicast filter-list 5

BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete Network      Next      Hop
Metric LocPrf Path

*>192.168.88.0 0.0.0.0      32768 ?
Total number of prefixes 1 QTECH# show ip bgp cidr-only
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Path

*>i64.12.0.0/16          0          i
192.168.195.183
100

*>i172.16.0.0/24         0          i
192.168.195.183
100

Total number of prefixes 2

QTECH# show bgp ipv4 unicast labels Network      Next Hop      In
Label/Out Label 1.1.1.1/32 192.167.1.1 17/18
1.1.1.2/32 192.167.1.1 no-label/19
```

Field	Description
Network	Route prefix
Nexthop	Nexthop IP address of the route
In label	Label assigned by this router (if any).
Out label	Label learnt from the nexthop router (if any).

Related Commands

Command	Description
show ip bgp	Displays the IPv4 unicast route information of BGP.

Platform Description

None

5.133. show bgp ipv4 unicast dampening parameters

Use this command to display the IPv4 unicast route dampening parameters configured for the BGP.

show bgp ipv4 unicast [vrf *vrf-name*] dampening parameters

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the IPv4 unicast route dampening parameters configured for BGP.

The following example displays the IPv4 unicast route dampening parameters configured for the BGP.

Configuration Examples

```
QTECH(config-router)# bgp dampening 25 10000 10000 200 QTECH# show bgp ipv4 unicast
dampening parameters dampening 25 10000 10000 200

Dampening Control Block(s): Reachability Half-Life time : 25 min Reuse penalty : 10000
Suppress penalty      : 10000 Max suppress time : 200 min
Max penalty (ceil)   : 29800000
Min penalty (floor)  : 5000
```

Related**Commands**

N/A

Platform Description

None

5.134. show bgp ipv4 unicast neighbors

Use this command to display the related information of BGP IPv4 unicast neighbor.

show bgp ipv4 unicast [vrf *vrf-name*] neighbors *neighbor-address*

Parameter	Description
<i>vrf-name</i>	VRF name
<i>neighbor-address</i>	Neighbor IPv4 address
neighbors <i>neighbor-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>neighbor-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)

Parameter Description

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to view the information of the connection with BGP IPv4 unicast neighbor.

Configuration Examples

The following example displays the related information of BGP IPv4 unicast neighbor.

QTECH# show bgp ipv4 unicast neighbors

BGP neighbor is 192.168.195.183, remote AS 23, local AS 23, internal link BGP version 4, remote router ID 44.0.0.1

BGP state = Established, up for 00:06:37

Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds Neighbor capabilities:

Route refresh: advertised and received (old and new) Address family IPv4 Unicast: advertised and received Graceful restart: advertised and received

Remote Restart timer is 120 seconds

Received 14 messages, 0 notifications, 0 in queue open message:1 update message:4 keepalive message:9 refresh message:0 dynamic cap:0 notifications:0 Sent 12 messages, 0 notifications, 0 in queue

open message:1 update message:3 keepalive message:8 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0

Minimum time between advertisement runs is 0 seconds For address family: IPv4 Unicast

BGP table version 2, neighbor version 1 Index 2, Offset 0, Mask 0x4

5. BGP4 Commands

Inbound soft reconfiguration allowed

8 accepted prefixes

0 announced prefixes

Connections established 2; dropped 1

Local host: 192.168.195.239, Local port: 1074

Foreign host: 192.168.195.183, Foreign port: 179

Nexthop: 192.168.195.239

Nexthop global: ::

Nexthop local: ::

BGP connection: non shared network

Last Reset: 00:06:43, due to BGP Notification sent Notification Error Message: (Cease/Unspecified Error Subcode) Using BFD to detect fast fallover

Related Commands

N/A

Platform Description

None

5.135. show bgp ipv4 unicast paths

Use this command to display the path information of the IPv4 unicast in the route database.

show bgp ipv4 unicast [*vrf vrf-name*] **paths**

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to view the path information in the route database.

The following example displays the path information of the IPv4 unicast in the route database.

Configuration Examples

```
QTECH# show bgp ipv4 unicast paths Address Refcnt Path
[0x1d7806a0:0] (67)
[0x1d7389a0:13] (20) 10
```

Related Commands

N/A

Platform Description

None

5.136. show bgp ipv4 unicast summary

Use this command to display the related information of BGP IPv4 unicast.

show bgp ipv4 unicast [vrf *vrf-name*] summary

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the related information of BGP IPv4 unicast.

The following example displays the related information of BGP IPv4 unicast.

```
QTECH # show bgp ipv4 unicast summary
BGP router identifier 192.168.183.1, local AS number 23 BGP table version is 2
2 BGP AS-PATH entries
1 BGP community entries
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 192.168.195.79 4 24 0
0 0 0 0 never Active
192.168.195.183 4 23 17 15 1 0 0 00:09:04 8
Total number of neighbors 2
```


Configuration Examples

Related Commands

Command	Description
router bgp	Enables the BGP protocol

Platform

Description None

5.137. show bgp ipv4 unicast update-group

Use this command to display information about an update-group in the BGP IPv4 unicast address family. **show bgp ipv4 unicast** [*vrf vrf-name*] **update-group** [*neighbor-address* | *update-group-index*] [**summary**]

Parameter Description

Parameter	Description
<i>vrf-name</i>	Specifies a VRF instance name.
<i>neighbor-address</i>	Specifies a neighbor that belongs to an update-group whose information needs to be displayed.
<i>update-group-index</i>	Specifies an update-group whose information needs to be displayed.
summary	Displays neighbor-related information.

Command Mode

Privileged EXEC mode

Default Level

14

Configuration Example

The following example displays information about an update-group in the BGP IPv4 unicast address family.

```
QTECH#show bgp ipv4 update-group
```

```
BGP version 4 update-group 1(ref 2), internal, Address Family: IPv4 Unicast Update
message formatted 2, replicated 2
```

```
Minimum route advertisement interval is 0 seconds Minimum AS origination interval is 1
seconds Format state: Current working
```

```
Refresh blocked Has 1 members:
```

```
192.168.195.183
```

The following example displays the neighbor summary of update-group 1 in the BGP IPv4 unicast address family.

```
QTECH # show bgp ipv4 unicast update-group 1 summary
```

```
BGP router identifier 192.168.183.1, local AS number 23 BGP table version is 2
```

```
2 BGP AS-PATH entries
```

```
1 BGP community entries
```

```
State/PfxRcd
```

```
192:168:195::79      4      24    0    0    0    0    0    never    Active
```

```
192:168:195::183 4 23      17    15    1    0    0    00:09:04    8
```

```
Total number of neighbors 2
```

Field description:

Field	Description
BGP router identifier	BGP router ID
local AS number	Local AS number of BGP
BGP table version	Version of the BGP routing table
BGP AS-PATH entries	Number of AS path entries
BGP community entries	Number of community attribute entries
Neighbor	Peer address
V	Protocol version
AS	Peer AS number

MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	Status of the neighbor state machine or number of received routing entries

5.138. show bgp ipv6 unicast

Use this command to display the IPv6 unicast routing information of BGP.

show bgp ipv6 unicast [*vrf vrf-name*] [*ipv6-prefix* [**longer-prefixes**]]

show bgp ipv6 unicast [*vrf vrf-name*] **community** *community-number* [**exact-match**]

show bgp ipv6 unicast [*vrf vrf-name*] **community-list** *community-name* [**exact-match**]

show bgp ipv6 unicast [*vrf vrf-name*] **extcommunity-list** *extcommunity-name*

show bgp ipv6 unicast [*vrf vrf-name*] **dampening** *dampened-paths* **show bgp ipv6**

unicast [*vrf vrf-name*] **dampening** *flap-statistics* **show bgp ipv6 unicast** [*vrf vrf-*

name] **filter-list** *path-list-number* **show bgp ipv6 unicast** [*vrf vrf-name*] **inconsistent-as**

show bgp ipv6 unicast [*vrf vrf-name*] **prefix-list** *ipv6-prefix-list-name*

show bgp ipv6 unicast [*vrf vrf-name*] **quote-regexp** *regexp* **show bgp ipv6 unicast**

[*vrf vrf-name*] **regexp** *regexp* **show bgp ipv6 unicast** [*vrf vrf-name*] **route-map** *map-*
tag

show bgp ipv6 unicast [*vrf vrf-name*] **neighbors** [*neighbor-address* [**received-routes** |
routes | **advertised-routes** | **policy** [**detail**]]]

Parameter Description

Parameter	Description
vrf-name	VRF name
IPv6-prefix	Displays the IPv6 routing information included in the specified network. The input format of the routing information prefix is X:X:X:X::X/<0-128>.
longer-prefixes	Displays the route map information.
	Displays the routing information including the

community community-number	specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
community-list community-name	Displays the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matches the community value or community-list.
extcommunity-list extcommunity-name	Displays the routing information including the specified extcommunity value.
dampening dampened-paths	Displays the restrained routing information.
dampening flap-statistics	Displays the routing dampening statistics.
filter-list <i>path-list-number</i>	Displays the routing information matching the filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.
prefix-list <i>ipv6-prefix-list-name</i>	Displays the routing information matching the specified prefix-list.
quote-regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp.
route-map <i>map-tag</i>	Displays the routing information matching the specified route-map filtering condition.

neighbors [<i>neighbor-address</i>]	Displays the BGP IPv6 unicast neighbor information.
neighbors <i>neighbor-address</i> received-routes	Displays all routing information received from the specified peer (including accepted and refused routes).
neighbors <i>neighbor-address</i> routes	Displays all the routing information received from the peer and accepted.
neighbors <i>neighbor-address</i> advertised-routes	Displays all the routing information sent to the specified peer.
neighbors <i>neighbor-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>neighbor-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to view the IPv6 unicast route information of BGP. You can filter the information with the specified parameter to display the matching route information. The function and use of this command is similar to the **show bgp ipv4 unicast** command, please refer to the command.

Configuration Examples

N/A

Related Commands

Command	Description
---------	-------------

show bgp ipv4 unicast	Displays the IPv4 unicast route information of BGP.
------------------------------	---

Platform Description

None

5.139. show bgp ipv6 unicast dampening parameters

Use this command to display the IPv6 unicast route dampening parameters configured for BGP.

show bgp ipv6 unicast [vrf *vrf-name*] dampening parameters

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the IPv6 unicast route dampening parameters configured for the BGP. The function and use of this command are similar to the **show bgp ipv4 unicast dampening parameters** command. Please refer to the command.

Configuration Examples

N/A

Related Commands

Command	Description
show bgp ipv4 unicast dampening parameters	Displays the IPv4 unicast route dampening parameters configured for BGP.

Platform**Description** None

5.140. show bgp ipv6 unicast neighbors

Use this command to display the related information of BGP IPv6 unicast neighbor.

show bgp ipv6 unicast [*vrf vrf-name*] **neighbors** *neighbor-address*

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name
<i>neighbor-address</i>	Neighbor IPv6 address.
neighbors <i>neighbor-address</i> policy	Related route policy information of BGP neighbor. (General)
neighbors <i>neighbor-address</i> policy detail	Related route policy information of BGP neighbor. (Detail)

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to view the information of the connection with BGP IPv6 unicast neighbor. The function and use of this command are similar to the **show bgp ipv4 unicast neighbors**

neighbor-address command. Please refer to the command.

Configuration Examples

N/A

Related Commands

Command	Description
show bgp ipv4 unicast neighbors <i>neighbor-address</i>	Displays the related information of BGP IPv4 unicast neighbor.

Platform

Description None

5.141. show bgp ipv6 unicast paths

Use this command to display the path information of the IPv6 unicast in the route database.

show bgp ipv6 unicast [vrf *vrf-name*] paths

Parameter Description

Parameter	Description
vrf-name	VRF name

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to view the path information in the route database.

```
QTECH# show bgp ipv6 unicast paths Address Refcnt Path
[0x1d7806a0:0] (67)
[0x1d7389a0:13] (20) 10
```

The following example displays the path information of the IPv6 unicast in the route database.

Configuration Examples

Related Commands

Command	Description
show bgp ipv4 unicast paths	Displays the path information of the IPv4 unicast in the route database.

Platform Description

None

5.142. show bgp ipv6 unicast summary

Use this command to display the related information of BGP IPv6 unicast.

show bgp ipv6 unicast [vrf *vrf-name*] summary

Parameter Description

Parameter	Description
vrf-name	VRF name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the related information of BGP IPv6 unicast. The function and use of this command are similar to the show bgp ipv4 unicast summary command. Please refer to the command.

Configuration Examples

N/A

Related Commands

Command	Description
router bgp	Enables the BGP protocol
show bgp ipv4 unicast summary	Displays the related information of BGP IPv4 unicast.

Platform Description

None

5.143. show bgp ipv6 unicast update-group

Use this command to display information about an update-group in the BGP IPv6 unicast address family. **show bgp ipv6 unicast** [*vrf vrf-name*] **update-group** [*neighbor-address* | *update-group-index*] [**summary**]

Parameter Description

Parameter	Description
<i>vrf-name</i>	Specifies a VRF instance name.
<i>neighbor-address</i>	Specifies a neighbor that belongs to an update-group whose information needs to be displayed.
<i>update-group-index</i>	Specifies an update-group whose information needs to be displayed.
summary	Displays neighbor-related information.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to display information about an update-group in the BGP IPv6 address family.

Configuration Example

The following example displays information about an update-group in the BGP IPv6 unicast address family.

```
QTECH#show bgp ipv6 update-group
```

```
BGP version 4 update-group 1(ref 2), internal, Address Family: IPv6 Unicast Update message  
formatted 2, replicated 2
```

```
Minimum route advertisement interval is 0 seconds Minimum AS origination interval is 1  
seconds Format state: Current working
```

```
Refresh blocked Has 1 members:
```

```
192:168:195::183
```

The following example displays the neighbor summary of update-group 1 in the BGP IPv6 unicast address family.

```
QTECH # show bgp ipv6 unicast update-group 1 summary BGP router identifier 192.168.183.1,
```

```
local AS number 23 BGP table version is 2
```

```
2 BGP AS-PATH entries
```

```
1 BGP community entries
```

```
Neighbor      AS MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down
State/PfxRcd
192:168:195::79      4      24      0      0      0      0      0      never  Active
192:168:195::183 4 23      17      15      1      0      0      00:09:04  8
Total number of neighbors 2
```

Field description:

Field	Description
BGP router identifier	BGP router ID
local AS number	Local AS number of BGP
BGP table version	Version of the BGP routing table
BGP AS-PATH entries	Number of AS path entries
BGP community entries	Number of community attribute entries
Neighbor	Peer address
V	Protocol version
AS	Peer AS number
MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	Status of the neighbor state machine or number of received routing entries

Prompt

N/A

Platform Description

N/A

5.144. show bgp l2vpn

Use the following command to display the BGP L2VPN routing information.

```
show bgp l2vpn { evpn } all
```

Use the following command to display the neighbor information of the BGP L2VPN EVPN address family.

```
show bgp l2vpn evpn all { ethernet-ad | ethernet-segment | inclusive-multicast | ip-prefix |  
mac-ip } [ detail ]
```

Use the following command to display the second type routing information of the BGP L2VPN EVPN address family.

```
show bgp l2vpn evpn all mac-ip mac_addr [ ip_addr [ detail ] | ipv6_addr [ detail ] |  
detail ]
```

Use the following command to display the fifth type routing information of the BGP L2VPN EVPN address family.

```
show bgp l2vpn evpn all ip-prefix { ip_addr [ detail ] | ipv6_addr [ detail ] | detail }
```

Use the following command to display the neighbor information of the BGP L2VPN address family.

```
show bgp l2vpn { evpn } all neighbor [ peer-address [ policy [ detail ] ] ]
```

Use the following command to display the neighbor summary information of the BGP L2VPN address family.

```
show bgp l2vpn { evpn } all summary
```

Use the following command to display the L2VPN EVPN information on the specified RD.

```
show bgp l2vpn evpn rd vpn_rd [[ethernet-ad | ethernet-segment | inclusive-multicast | ip-  
prefix |  
mac-ip ] [ detail ]]
```

Use the following command to display the L2VPN EVPN information on the specified EVI.

```
show bgp l2vpn evpn evi vni-id [ [ ethernet-ad | ethernet-segment | inclusive-multicast | ip-  
prefix  
| mac-ip ] [ detail ] ]
```

Parameter	Description
evpn	Displays EVPN information.
all	Displays all NLRI information that contains the VPLS instance or the VPWS instance.
<i>ve_id:offset</i>	Displays the VFI instance information of the specified ve_id:offset
ethernet-ad [detail]	Displays basic (detailed) information of the first type of BGP L2VPN EVPN routes.
ethernet-segment [detail]	Displays basic (detailed) information of the fourth type of BGP L2VPN EVPN routes.
inclusive-multicast [detail]	Displays basic (detailed) information of the third type of BGP L2VPN EVPN routes.
ip-prefix [detail]	Displays basic (detailed) information of the fifth type of BGP L2VPN EVPN routes.
ip-prefix [<i>ip_addr</i> [detail]] <i>ipv6_addr</i> [detail] detail]	Displays basic (detailed) information of routes with specific IP address or IPv6 address in the fifth type of BGP L2VPN EVPN routes.
mac-ip [detail]	Displays basic (detailed) information of the second type of BGP L2VPN EVPN routes.
mac-ip <i>mac_addr</i> [<i>ip_addr</i> [detail]] <i>ipv6_addr</i> [detail] detail]	Displays basic (detailed) information of routes with specific MAC addresses or MAC addresses+IP addresses/IPv6 addresses in the second type of BGP L2VPN EVPN routes.

neighbor [<i>peer-address</i>]	Displays the BGP L2VPN neighbor information. You can specify the specific neighbor information by entering the parameter <i>neighbor-address</i> . Otherwise all BGP L2VPN neighbor information is displayed.
neighbor <i>peer-address</i> policy	Displays the summarized routing policy information on BGP neighbor.
neighbor <i>peer-address</i> policy detail	Displays the detailed routing policy information BGP neighbor,
summary	Displays main BGP L2VPN information, including site ID, OFFSET, LABEL BASE and NEXT HOP.
rd <i>vpn_rd</i>	The specified RD.
vfi <i>vfi_name</i>	The specified VFI instance.
evi <i>vni-id</i>	The specified evl instance.

Parameter Description

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

The following example displays all L2VPN EVPN address family routing information.

```
QTECH(config)# show bgp l2vpn evpn all
BGP table version is 16, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric          LocPrf          Weight Path Route
Distinguisher: 1:100 (Default for EVI 1122)
```

```
*> 0:32:1.1.1.1/72 0.0.0.0 32768 i

Total number of prefixes 1
Route Distinguisher: 1.1.1.1:100 (Default for EVI 100)
*> 0:6:0011.2233.2016:0:0.0.0.0/128
      0.0.0.0 32768 i
*>i0:6:00d0.f822.33df:0:0.0.0.0/128
      2.2.2.2 0 100 0 i
*> 0:6:0011.2233.2016:32:100.1.1.2/128
      0.0.0.0 32768 i
*>i0:6:00d0.f822.33df:32:100.1.1.1/128
      2.2.2.2          0          100          0 i
*> 0:32:1.1.1.1/72 0.0.0.0          32768 i
*>i0:32:2.2.2.2/72 2.2.2.2          0          100          0 i

Total number of prefixes 6
```

Configuration Examples

Command	Description
BGP table version	BGP table version.
Local Router ID	Local Router ID. Generally it is a loopback address.
status codes	Status codes: s :The route is dampened. d :Shielded route flap. h: Historical routes that no longer available * : Valid routes > : Optimal routes i : IBGP routes r : Fails to install the RIB routing table. S: Old routes.
Origin Codes	Origin Codes: i: IGP. e: EGP. ?: Incomplete.
Network	Routing information in the form aa:bb. The aa here represents site ID and the bb represents label model offset.

Next hop	Next hop IP address.
Metric	Metric value of the represent route (if be displayed.)
LocPrf	Local priority.
Path	AS path that reach the destination network.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.145. show bgp l2vpn update-group

Use this command to display the update-group information of BGP L2VPN address family.

```
show bgp l2vpn { evpn } all update-group [ neighbor-address | update-group-index ]
[ summary ]
```

Parameter Description

Parameter	Description
evpn	Displays the L2VPN EVPN address family information.
<i>neighbor-address</i>	Displays the update-group information of specified neighbor.
<i>update-group-index</i>	Display the specified update-group information.
summary	Display neighbor information.

Defaults

N/A

Command Mode

Usage Guide

Display the update-group information of BGP L2VPN address family.

The following example displays the update-group information of BGP L2VPN EVPN address family

Configuration Examples

```
QTECH#show bgp l2vpn evpn all update-group
BGP version 4 update-group 1(ref 2), internal, Address Family: L2VPN EVPN
Update message formatted 2, replicated 2
Minimum route advertisement interval is 0 seconds
Minimum AS origination interval is 1 seconds
Refresh blocked Has 1 members:
192.168.195.183
```

The following example displays the neighbor summary of update-group 1 of BGP L2VPN EVPN address family

```
QTECH # show bgp l2vpn evpn all update-group 1 summary
BGP router identifier 192.168.183.1, local AS number 23
BGP table version is 2
2 BGP AS-PATH entries
1 BGP community entries
Neighbor      V    AS  MsgRcvd MsgSent TblVer  InQ  OutQ  Up/Down
State/PfxRcd
192.168.195.79 4    24    0        0        0    0    0    never
Active
192.168.195.183 4    23    17       15        1    0    0    00:09:04
8
Total number of neighbors 2
```

Field	Description
BGP router identifier	BGP router ID
local AS number	Local AS number of BGP
BGP table version	Version of the BGP routing table
BGP AS-PATH	Number of AS path entries

entries	
BGP community entries	Number of community attribute entries
Neighbor	Peer address
V	Protocol version
AS	Peer AS number
MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	Status of the neighbor state machine or number of received routing entries

Platform Description

N/A

5.146. show bgp statistics

Use this command to display the BGP statistics information.

show bgp statistics [vrf *vrf-name*]

Parameter Description

Parameter	Description
vrf <i>vrf-name</i>	Displays the BGP statistics information of VRF.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Without the **vrf** parameter, the global BGP statistics information will be displayed.

The following example displays the BGP statistics information.

```
QTECH#show bgp statistics Local as 100, Router id 1.1.1.1
Total neighbor 10, Established neighbor 9, Admin-Down neighbor 1
IBGP neighbor 8, Established IBGP neighbor 8, Admin-Down IBGPneighbor
0
EBGP neighbor 2, Established EBGP neighbor 1, Admin-Down EBGPneighbor
1
AS-PATH entries 1, Community entries 1, Extended-Community entries 0

For address family: IPv4 Unicast
Activated neighbor 9, Unactivated neighbor 0 Activated IBGP neighbor 8, Unactivated IBGP
neighbor 0 Activated EBGP neighbor 1, Unactivated EBGP neighbor 0

For address family: IPv6 Unicast
Activated neighbor 0, Unactivated neighbor 9
Activated IBGP neighbor 0, Unactivated IBGP neighbor 0 Activated EBGP neighbor 0,
Unactivated EBGP neighbor 0
```

Configuration Examples

Parameter	Description
Router id	ID of BGP router.
Total neighbor	Total number of neighbors.
Established neighbor	Number of UP neighbors.
Admin-Down neighbor	Number of admin down neighbors.
IBGP neighbor	Number of IBGP neighbors.
Established IBGP neighbor	Number of UP IBGP neighbors.
Admin-Down IBGP neighbor	Number of admin down IBGP neighbors.
EBGP neighbor	Number of EBGP neighbors.
AS-PATH entries	Number of AS-PATH entries.
Community entries	Number of community entries.
Extended-Community	Number of extended community entries.
Established EBGP neighbor	Number of UP EBGP neighbors.

Admin-Down EBGp neighbor	Number of admin down EBGp neighbors.
Activated neighbor	Number of activated neighbors.
Unactivated neighbor	Number of unactivated neighbors, not including UP neighbors.
Activated IBGP neighbor	Number of activated IBGP neighbors.
Unactivated IBGP neighbor	Number of unactivated IBGP neighbors, not including UP neighbors.
Activated EBGp neighbor	Number of activated EBGp neighbors.
Unactivated EBGp neighbor	Number of unactivated EBGp neighbors, not including UP neighbors.

Platform Description

N/A

5.147. show evpn

Use this command to display the EVI instance.

show evpn [*vni-id* [detail] / detail]

Parameter Description

Parameter	Description
<i>vni-id</i>	Indicates the ID of specified EVI instance.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

If an ID of EVI instance is exported, display the information of the EVI. IF no EVI ID is imported, display all EVIs' information.

The following example displays all information of EVI 100.

Configuration Examples

```
Import VPN route-target communities RT: 100:100(auto)
Export VPN route-target communities RT: 100:100(auto)
EVI Layer 3 Interface: OverlayRouter 100 All Route count: 6
Ethernet Auto-discovery Route count: 0 MAC/IP Advertisement Route count: 4
Inclusive Multicast Ethernet Tag Route count: 2 Ethernet Segment Route count: 0
Install Route count: 3
```

Parameter	Description
RD	RD value of EVI.
EVI Layer 3 Interface	L3 interface associated with EVI.
Export VPN route-target communities	Value of the exported RT of EVI.
Import VPN route-target communities	Value of the imported RT of EVI.
Route count	Number of routes in EVI instance.

The following example displays key information of EVI.

```
QTECH#show evpn
vni    rd      interface
-----
100    1.1.1.1:100  OverlayRouter  10
                                0
300    1.1.1.1:300  N/A
789    1.1.1.1:789  N/A
1000   1.1.1.1:1000 OverlayRouter  10
                                00
1122   1:100       N/A
```

```

2000      1.1.1.1:2000      OverlayRouter      20
                                     00

3344      1.1.1.1:3344      N/A

1678889   1.1.1.1:40489     N/A

Total number: 8

```

Parameter	Description
vni	vni-id of EVI.
rd	RD value of EVI
interface	L3 interface associated with EVI.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.148. show evpn mac

Use this command to display the mobilized or conflict MAC information

show evpn mac {conflict | mobility} [vni-id]

Parameter Description

Parameter	Description
conflict	Display the conflicted MAC
mobility	Display the mobilized MAC
<i>vni-id</i>	Display the ID of specific EVI instance

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

If the parameter has EVI ID, then display the MAC information of specific EVI; if no EVI ID is entered, display the MAC information of all EVI.

```
QTECH#show evpn mac mobility
vni    mac                count  remain-time 10 0055.1000.0004 2
72
10     0055.1000.000a     1      66
10     0055.1000.000e     1      72
10     0055.1000.0013     1      27
10     0055.1000.0015     4      75
```

The following example checks the mobilized MAC information.

Parameter	Description
vni	VNI-ID of EVI.
mac	Mobilized MAC address
count	Mobility times
remain-time	Remaining time of the timer for conflict. Unit: second.

Configuration Examples

```
QTECH#show evpn mac conflict QTECH#show evpn mac
conflict
vni mac seq retry-time
10     0011.0011.e69c     6 -----
```

The following example checks the conflict MAC information.

Parameter	Description
vni	vni-id of EVI.
mac	Mobilized MAC address
seq	Sequence number of conflict MAC address
Retry-time	Remaining time for retry. Unit: second

Related Commands

Command	Description
N/A	N/A

Platform

Description

N/A

5.149. show ip bgp

Use this command to display the BGP IPv4 unicast address families' route information. The method of use is the same as other BGP show commands.

`show ip bgp [vrf vrf-name] [network [network-mask [longer-prefixes]] | cidr-only | community`

`[community-number [exact-match]] | filter-list path-list-number | community-list community-name [exact-match] | regexp regexp | quote-regexp regexp | extcommunity-list extcommunity-name | inconsistent-as | prefix-list ip-prefix-list-name | route-map map-tag]`
Display route flap's parameters.

`show ip bgp [vrf vrf-name] dampening { flap-statistics | dampened-paths | parameters }`
Display neighbors' related information.

`show ip bgp [vrf vrf-name] neighbors [peer-address [received-routes | routes | advertised-routes [policy [detail]]]]`

`show ip bgp [vrf vrf-name] summary`

Display directory information. `show ip bgp [vrf vrf-name] paths` Display route scan status.

`show ip bgp scan`

Display related information under VRF.

`show ip bgp { vrf vrf-name | labels }`

Display related information of BGP IPv4 unicast update-group.

`show ip bgp [vrf vrf-name] update-group [neighbor-address | update-group-index] [summary]`

Parameter Description

Parameter	Description
vrf-name	VRF name.
network	Displays specific route information in the route table.

network-mask		<i>Displays route information in the specific network.</i>
longer-prefixes		<i>Displays the route map information.</i>
cidr-only		<i>Displays route information without specific category.</i>
community community-number		<i>Displays route information containing specific community value. The community-number is the group number. The format is AA:NN (autonomous system number/2-byte figure), or the following pre-defined value: internet, no-export, local-as or no-advertise.</i>
community-list community-name		<i>Displays the BGP route information of the specified community list. The community-name is the name of the community list.</i>
dampening dampened-paths		<i>Displays dampened route information.</i>
dampening statistics	flap-	<i>Displays the route flap statistics.</i>
dampening parameters		<i>Displays believed route flap parameters.</i>
extcommunity-list extcommunity-name		<i>Displays route information containing specific extcommunity value.</i>
filter-list number	path-list-	<i>Displays the route information that complies with the filter list. The</i>
		<i>path-list-numbe is the marking number of the filter list.</i>
inconsistent-as		<i>Displays the route information of inconsistent source AS.</i>
Labels		<i>Displays the IPv4 label route information.</i>
neighbors	peer-	<i>Displays the route information of BGP neighbors.</i>

<i>address</i>		
neighbors <i>address</i> received-routes	<i>peer-</i>	Displays all routing information received from the specified peer (including accepted and refused routes).
neighbors <i>address</i> routes	<i>peer-</i>	Displays all the routing information received from the peer and accepted.
neighbors <i>address</i> advertised-routes	<i>peer-</i>	Displays all the routing information sent to the specified peer.
neighbors <i>address</i> policy	<i>peer-</i>	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>address</i> policy detail	<i>peer-</i>	Displays the related routing policy information of BGP neighbors. (Detail)
Paths		Displays the route information in the route database.
prefix-list		Displays the route information that complies with the prefix list.
quote-regexp <i>regexp</i>		Displays the BGP route information of regular expression in the specified double quotation mark of the AS route attribute.
regexp <i>regexp</i>		Displays the BGP route information of specified regular expression of the AS route attribute.
route-map		Displays the route information that complies with the route map.
Scan		Displays the BGP route scanning status.
summary		Displays related information of BGP neighbors.

update-group [<i>neighbor-address</i> <i>update-group-index</i>]	Display update-group information. When <i>neighbor-address</i> is specified, display the update-group information of the specified neighbor. When <i>update-group-index</i> is specified, display the specified update-group information.
--	---

Defaults -

Command Mode

Privileged EXEC mode

Usage Guide

The show ip bgp command is the same as show bgp ipv4 unicast in terms of the function. All the parameters in show bgp ipv4 unicast apply to show ip bgp.

Configuration Examples

Configuration Examples

Command	Description
show bgp ipv4 unicast	Displays IPv4 unicast route information in BGP route information.

Platform -Description

5.150. vni

Parameter Description

Use this command to create an EVI instance. Use the no form of this command to delete the EVI instance. Use the default form of this command to restore the default settings.

vni *vni-id*

no vni *vni-id*

default vni *vni-id*

Parameter	Description
<i>vni-id</i>	Indicates the VNI ID. Ranges from 1 to 16777215.

Defaults **N/A****Command****Mode**

EVPN configuration mode

Usage Guide

Configure the EVPN mode first, and then enter the evpn-vni configuration mode. Run exit command to exit.

Configuration Examples

The following example configures an EVI instance in EVPN mode.

```
QTECH(config)# evpn
QTECH(config-evpn)# vni 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.151. vni range

Use this command to create EVI instances in batches and enter the EVI instance batch configuration mode. Use the no form of this command to delete EVI instances in batches. Use the default form of this command to restore the default settings.

vni range *vni-id-list*

no vni range *vni-id-list*

default vni range *vni-id-list*

Parameter Description

Parameter	Description
<i>vni-id-list</i>	Name of the VNI ID list

Defaults

N/A

Command Mode

EVPN configuration mode.

Default Level

14

Usage Guide

The configuration fails if the number of configured VNI instances exceeds the capacity or a VNI instance is being deleted.

The RD values of different VNI instances must be different. Therefore, only the automatic RD configuration mode is available for configuring VNI instances in batches, and VNI instances

cannot be configured manually.

Configuration Examples

```
QTECH(config)# evpn
QTECH(config-evpn)# vni range 100,200-300
QTECH(config-evpn-vni-range)#
```

The following example configures EVI instances in batches in EVPN configuration mode.

Verification Run the **show running-config** command to display the EVPN configurations.

Prompts

1. The following error information is displayed if the number of VNI instances exceeds the capacity.

```
%thisrangeconfigurationmaybeyondvnicapacity(8000).pleasecheckyourinput
```

2. The following error information is displayed if a VNI instance is being deleted.

```
% evpn evi 100 is deleting, Fail to configure vnirange.
```

6. PBR COMMANDS

6.1. clear ip pbr statistics

Use this command to clear the IPv4 PBR forwarded packet count.

clear ip pbr statistics [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the
	device clears the IPv4 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv4 PBR forwarded packet count on every interface where IPv4 PBR is enabled.
local	Clears the IPv4 PBR forwarded packet count on the local interface.

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to clear the IPv4 PBR forwarded packet count.

Configuration Examples

Related Commands

Platform Description

The following example clears the IPv4 PBR forwarded packet count.

```
QTECH#clear ip pbr statistics
```

Command	Description
N/A	N/A

N/A

6.2. clear ipv6 pbr statistics

Use this command to clear the IPv6 PBR forwarded packet count.

clear ipv6 pbr statistics [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the device clears the IPv6 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv6 PBR forwarded packet count on every interface where IPv6 PBR is enabled.
local	Clears the IPv6 PBR forwarded packet count on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to clear the IPv6 PBR forwarded packet count.

Configuration Examples

The following example clears the IPv6 PBR forwarded packet count.

```
QTECH#clear ipv6 pbr statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.3. ip local policy route-map

Parameter Description

Use this command to apply the policy-based routing (PBR) on the packets sent locally. Use the **no**

form of this command to restore the default setting.

ip local policy route-map *route-map*

no ip local policy route-map

Parameter	Description
<i>route-map-name</i>	Name of the route map

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

Configuration Examples

The following examples send the packets with the source address 192.168.217.10 from the serial 2/0. The following example defines an ACL that match the IP packet.

```
QTECH(config)#access-list 1 permit 192.168.217.10
```

The following example defines the route map.

```
Qtech(config)#route-map lab1 permit 10
Qtech(config-route-map)#match ip address 1
Qtech(config-route-map)#set interface serial 2/0
Qtech(config-route-map)#exit
```

The following example applies PBR on the local interface.

```
QTECH(config)#ip local policy route-map lab1
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the output port of the policy-based routing.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.

set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description

N/A

6.4. ip policy

Use this command to set the policy: redundant backup or load balancing used between multiple next hops of the PBR applied for the **set ip [default] nexthop** command in global configuration mode. Use the **no** form of this command to restore the default setting.

ip policy { load-balance | redundance } no ip policy

Parameter Description

Parameter	Description
load-balance redundance	Specifies the policy: load balancing or redundant backup.

Defaults

Redundant backup is adopted by default.

Command Mode

Global configuration mode

Usage Guide

When you configure the **set ip next-hop** command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop of the policy-based routing takes effect. When the load balancing is set, multiple resolved next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops. The resolved next hop refers to the ARP message learned by the next hop and the MAC address corresponding to this ARP exists in the MAC address table.

NPE80 does not support this command.

Configuration Examples

In the example below, there are multiple next hops configured in the route map. After the redundant backup is set in global configuration mode, only the first next hop among the sub-route map of the policy-based routing applied on the interface FastEthernet 0/0 takes effect.

The following example sets the ACL that match the IP packet.

```
QTECH(config)#access-list 1 permit 10.0.0.1
QTECH(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
QTECH(config)#route-map lab1 permit 10 QTECH(config-route-map)#match ip address 1
QTECH(config-route-map)#set ip next-hop 196.168.4.6 QTECH(config-route-map)#set ip next-
hop 196.168.4.7 QTECH(config-route-map)#set ip next-hop 196.168.4.8 QTECH(config-route-
map)#exit
QTECH(config)#route-map lab1 permit 20 QTECH(config-route-map)#match ip address 2
QTECH(config-route-map)#set ip next-hop 196.168.5.6 QTECH(config-route-map)#set ip next-
hop 196.168.5.7 QTECH(config-route-map)#set ip next-hop 196.168.5.8
QTECH(config-route-map)#exit
```

The following example applies the policy-based routing on the interface.

```
QTECH(config)#interface FastEthernet 0/0 QTECH(config-if)#ip policy route-map lab1
QTECH(config-if)#exit
QTECH(config)#ip policy redundancy
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.5. ip policy route-map

Parameter Description

Use this command to apply the policy-based routing on an interface. Use the **no** form of this command to restore the default setting.

ip policy route-map *route-map*

no ip policy route-map

Defaults This function is disabled by default.

Parameter	Description
<i>route-map</i>	Name of the route map

Command Mode

Interface configuration mode

Usage Guide

The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples

In the example below, when the interface FastEthernet0/0 receives a datagram, if the source address of the datagram is 10.0.0.1, it sets the next-hop as 196.168.4.6; if the source address is 20.0.0.1, it sets the next-hop as 196.168.5.6; otherwise, the general forwarding will be performed. The following example sets the ACL matched with the IP packets.

```
Qtech(config)#access-list 1 permit 10.0.0.1
Qtech(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
QTECH(config)#route-map lab1 permit 10 QTECH (config-route-map)#match ip address 1
QTECH(config-route-map)#set ip next-hop 196.168.4.6 QTECH(config-route-map)#exit
QTECH(config)#route-map lab1 permit 20 QTECH(config-route-map)#match ip address 2
QTECH(config-route-map)#set ip next-hop 196.168.5.6
QTECH(config-route-map)#exit
```

The following example applies the route map on the interface.

```
QTECH(config)#interface FastEthernet 0/0
QTECH(config-if)#ip policy route-map lab1 QTECH(config-if)#exit
```

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the policy-based routing output port.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description

N/A

6.6. ip policy-source in-interface

Parameter Description

Use this command to configure the source address policy-based routing for the IPv4 packets received on an interface. Use the no form of this command to disable the source address policy-based routing on the interface.

```
ip policy-source in-interface interface-type sequence { source-address mask |
source-address/mask } {[default] next-hop ip-address [weight] | }[default] interface
out-interface-type | vrf vrf-name}
no ip policy-source in-interface interface-type sequence [ {source-address mask | source-
address/mask} [ [default] next-hop ip-address [weight] | [default] interface out-interface-
type | vrf vrf-name ] ]
```

Parameter	Description
<i>interface-type</i>	Interface type
<i>sequence</i>	Policy sequence number. The lower the number is, the higher the
	priority is.
<i>source-address</i>	Source IPv4 address.
<i>mask</i>	Address mask.
<i>ip-address</i>	Next hop IPv4 address
<i>weight</i>	Next hop weight
<i>out-interface-type</i>	Type of the next hop interface
<i>vrf-name</i>	VRF instance name

Defaults

Source address policy-based routing is disabled by default.

Command Mode

Global configuration mode

Usage Guide

You can configure multiple `ip source-policy in-interface` commands on an interface. The policy with different source addresses must be configured with different sequence numbers. The lower the sequence number is, the higher the priority is.

In case of the same sequence number, the priority order of the next hop type is as follows:

```
vrf vrf-name > next-hop ip-address > interface out-interface-type > default next-hop ip-address >
```

```
default interface out-interface-type
```

The priority of the source address PBR is lower than that of the interface PBR.

Configuration Examples

In the example below, when the interface GigabitEthernet0/0 receives a datagram, if the source address of the datagram is 10.0.0.2, the next-hop is set as 196.168.1.2; otherwise, the general forwarding will be performed.

The following example configures source address PBR in global configuration mode.

```
Qtech(config)# ip source-policy in-interface gigabitEthernet 0/0 1 10.0.0.2
255.255.255.255 next-hop 196.168.1.2
Qtech(config)# ip source-policy in-interface gigabitEthernet 0/0 2 20.0.0.2
255.255.255.255 next-hop 196.168.2.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.7. ipv6 local policy route-map

Use this command to enable the policy-based routing on the packets sent locally. Use the `no` form of this command to restore the default setting.

```
ipv6 local policy route-map route-map-name
```

```
no ipv6 local policy route-map
```

Parameter Description

--	--

Parameter	Description
<i>route-map-name</i>	Name of the router map applied locally, which is configured by the router-map command.

Defaults

This function is disabled by default.

Command Mode

Global Configuration mode

Usage Guide

This command is valid only for the IPv6 packets in accordance with the policy (for example, ping packets used for management) sent locally, but not the packets received locally.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

Configuration Examples

The following examples display the PBR application process: The device sends the packets from the source address 2003:1000::10/80 to the 2001:100::/64, the packets will match ACL6 of aaa and be sent to the device 2003:1001::2.

The following example defines the ACL matched with the IPv6 packet:

```
QTECH(config)#ipv6 access-list aaa
QTECH(config)#permit ipv6 2003:1000::10/80 2001:100::/64

QTECH(config)#route-map pbr-aaa permit 10 QTECH(config-route-map)#match ipv6 address aaa
QTECH(config-route-map)#set ipv6 next-hop 2003::1001::2
```

- The following example defines the router map.
- The following example applies the PBR on the device.

```
QTECH(config)#ipv6 local policy route-map pbr-aaa
```


Related Commands

Command	Description
match ipv6 address	Sets the ACL6 used to match the IPv6 packets in the IPv6 PBR.
match length	Defines the length of matched packets.
route-map	Defines the route map for PBR.
set default interface	Defines the default next hop output port.
set interface	Defines the next hop output port.
set ipv6 default next-hop	Sets the default next hop of packet forwarding.
set ipv6 next-hop	Sets the next hop of packet forwarding.
set ipv6 precedence	Sets the priority field in the head of IPv6 packets.
show ipv6 policy	Displays the current PBR application.
show route-map	Displays the current router map configuration.

Platform Description

N/A

6.8. ipv6 policy

Parameter Description

Use this command to set the policy: redundant backup or load balancing, applied for the **set ip nexthop** command in global configuration mode. Use the **no** form of this command to restore the default setting.

ipv6 policy { load-balance | redundance } no ipv6 policy

Parameter	Description
load-balance	Sets the policy as load balancing.
redundance	Sets the policy as redundant backup.

Defaults

Redundant backup is adopted by default.

Command Mode

Global configuration mode

Usage Guide

This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

Configuration Examples

This function is valid for the multiple next-hops.

When you configure the set ip next-hop command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop takes effect. The second configured next hop will take effect only when the first one fails and the first next hop will take effect again if it recovers.

When the load balancing is set, multiple next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops.

The resolved next hop refers to the learned MAC address for the next-hop.

The following example sets load-balancing mode for multiple nexthops. The following example configures an ACL matching with IP packets.

```
QTECH(config)# ipv6 access-list 1
QTECH(config-ipv6-acl )# permit ipv6 1000::1 any QTECH(config)# ipv6 access-list 2
QTECH(config-ipv6-acl )# permit ipv6 2000::1 any
```

```

QTECH(config)# route-map lab1 permit 10 QTECH(config-route-map)# match ipv6 address 1
QTECH(config-route-map)# set ipv6 next-hop 2002::1 QTECH(config-route-map)# set ipv6
next-hop 2002::2 QTECH(config-route-map)# set ipv6 next-hop 2002::3 QTECH(config-route-
map)# exit

QTECH(config)# route-map lab1 permit 20 QTECH(config-route-map)# match ipv6 address 2
QTECH(config-route-map)# set ipv6 next-hop 2002::5 QTECH(config-route-map)# set ipv6
next-hop 2002::6 QTECH(config-route-map)# set ipv6 next-hop 2002::7
QTECH(config-route-map)# exit

```

The following example defines a route map.

The following example applies policy-based routing on the interface.

```

QTECH(config)# interface FastEthernet 0/0 QTECH(config-if)# ipv6 policy route-map lab1
QTECH(config-if)# exit

QTECH(config)# ipv6 policy load-balance

```

Related Commands

Command	Description
set ipv6 default next-hop	Defines the default next hop for forwarding the packets.
set ipv6 next-hop	Defines the next hop for forwarding the packets.
show ipv6 policy	Displays the current policy-based routing application.

Platform Description

N/A

6.9. ipv6 policy route-map

Use this command to apply the policy-based routing on an interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

ipv6 policy route-map *route-map-name*

no ip policy route-map

Parameter Description

Parameter	Description
<i>route-map-name</i>	Name of the PBR router map applied locally, which is configured by the router-map command.

Defaults

This function is disabled by default..

Command Mode

Interface configuration mode

Usage Guide

The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples

An IPv6 packet is received on the fastEthernet 0/0. If the packet is sent from

10::/64 network segment, it is forwarded to the next hop of 2000:1; if the

packet is sent from 20::/64 network segment, it is forwarded to the next hop of

2000:2 or forwarded as usual.:

The following example configures an ACL matched with the IP packet.

```
QTECH(config)# ipv6 access-list acl_for_pbr1 QTECH (config-ipv6-acl)# permit ipv6 10::/64
any QTECH(config)# ipv6 access-list acl_for_pbr2
QTECH (config-ipv6-acl)# permit ipv6 20::/64 any
```

```
QTECH(config)# route-map rm_pbr permit 10
QTECH (config-route-map)# match ipv6 address acl_for_pbr1 QTECH(config-route-map)# set
ipv6 next-hop 2000::1 QTECH(config-route-map)# exit
QTECH(config)# route-map rm_pbr permit 20
QTECH(config-route-map)# match ipv6 address acl_for_pbr2 QTECH(config-route-map)# set
ipv6 next-hop 2000::2 QTECH(config-route-map)# exit
```

The following example defines a route map.

The following example applies the route map to the interface.

```
QTECH(config)# interface FastEthernet 0/0 QTECH(config-if)# no switchport
QTECH(config-if)# ipv6 policy route-map rm_pbr
```

Related Commands

Platform Description

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

Command	Description
route-map	Defines the route map.
match ipv6 address	Sets the IPv6 ACL used to match the IPv6 packets in the IPv6 PBR.
set ipv6 default next-hop	Defines the default next hop of the packet forwarding.
set ipv6 next-hop	Defines the next hop of the packet forwarding.
show ipv6 policy	Displays the current policy-based routing application.
show route-map	Displays the current route map configurations.

N/A

6.10. ipv6 policy-source in-interface

Use this command to configure the source address policy-based routing for the IPv6 packets received on an interface. Use the **no** form of this command to disable the source address policy-based routing on the interface.

```
ipv6 policy-source in-interface interface-type sequence source-address/prefix-length
{[default]
next-hop ipv6-address [weight] }| [default] interface out-interface-type | vrf vrf-name}
no ipv6 policy-source in-interface interface-type sequence [ source-address/prefix-length
[ [default] next-hop ipv6-address [weight] ] | [default] interface out-interface-type | vrf vrf-name }
```

Parameter Description

Parameter	Description
<i>interface-type</i>	Interface type
<i>sequence</i>	Policy sequence number. The lower the number is, the higher the priority is.
<i>source-address</i>	Source IPv6 address.
<i>ipv6-address</i>	Next hop IPv6 address
<i>weight</i>	Next hop weight
<i>out-interface-type</i>	Type of the next hop interface
<i>vrf-name</i>	VRF instance name

Defaults

Source address PBR is disabled by default.

Command Mode

Global configuration mode

Usage Guide You can configure multiple ipv6 source-policy in-interface commands on an interface. The policy with different source addresses must be configured with different sequence numbers. The lower the sequence number is, the higher the priority is.

In case of the same sequence number, the priority order of the next hop type is as follows:
 vrf *vrf-name* > next-hop *ipv6-address* > interface *out-interface-type* > default next-hop *ipv6-address* > default interface *out-interface-type*

The priority of the source address PBR is lower than that of the interface PBR.

Configuration Examples

In the example below, when the interface GigabitEthernet0/0 receives an IPv6 datagram, if the source address of the datagram is in the network segment of 10::/64, the next-hop is set as 2000:1; if the source address of the datagram is in the network segment of 20::/64, the next-hop is set as 2000:2; otherwise, the general forwarding will be performed.

The following example configures source address PBR in global configuration mode

```
QTECH(config)# ipv6 source-policy in-interface gigabitEthernet 0/0 2
10::/64 next-hop 2000::1
QTECH(config)# ipv6 source-policy in-interface gigabitEthernet 0/0 2
20::/64
next-hop 2000::2
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.11. show ip pbr bfd

Use this command to display the correlation between the IPv4 policy router and BFD.

show ip pbr bfd

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```
QTECH# show ip pbr bfd
```

VRF ID	Ifindex	Host	State	Refcnt
0	13	192.168.8.100	Up	2

The following example displays the correlation between the IPv4 policy router and BFD.

Related Commands

Platform Description

Field Description

Field	Description
VRF ID	VRF of BFD neighbors correlated with the policy router
Ifindex	The interface index of BFD neighbors correlated with the policy router
Host	The peer IPv4 address
State	Up/Down status of BFD neighbors correlated with the policy router
Refcnt	Calculation referred by BFD neighbors

Command	Description
N/A	N/A

N/A

6.12. show ip pbr route

Use this command to display the IPv4 PBR information on the interface.

show ip pbr route [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv4 BPR information of this interface is displayed. Otherwise, the IPv4 BPR information of all interfaces where the IPv4 PBR is enabled is displayed.
local	Displays the IPv4 PBR information on the local interface

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the IPv4 PBR information.

Configuration Examples

```
QTECH#show ip pbr route PBR IPv4 Route Summay : 1
Interface      : GigabitEthernet 0/1
```

The following example displays the IPv4 PBR information on the interfaces.

```
Sequence      : 10
ACL[0]        : 2900
ACL_CLS[0]    : 0
Min Length    : None
Max Length    : None
VRF ID        : 0
```

```

Route Flags :
Route Type : PBR Direct : Permit
Priority : High
Tos_Dscp : None Precedence : None Tos_Dscp : 0
Precedence : 0
Mode : redundance Nexthop Count : 1
Nexthop[0] : 192.168.8.100
Weight[0] : 1
Ifindex[0] : 2

```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
Min Length	The minimum match length.
Max Length	The maximum match length.
VRF ID	Port-correlated VRF ID.
Route Flags	<p>PBR flag bit:</p> <p>Route Type: “PBR” indicates PBR routes. “Normal” indicates common routes.</p> <p>Direct: PBR matching action, permit or deny</p> <p>Priority: PBR priority, High or Low</p> <p>Tos_Dscp: Displays whether the tos rule or the dscp rule is configured.</p> <p>Precedence: Displays whether the set ip precedence rule is configured.</p>
Mode	Specifies the redundancy mode or the next hop load balancing mode.
Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.

Nexthop	Specifies the next hop IP address.
Weight	Specifies the next hop weight.
Ifindex	Specifies the outbound interface index corresponding to the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.13. show ip pbr route-map

Use this command to display the IPv4 PBR route-map information.

show ip pbr route-map *route-map-name*

Parameter Description

Parameter	Description
<i>route-map-name</i>	The route-map name.

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the IPv4 PBR route-map information.

```
QTECH#show ip pbr route-map rm Pbr VRF:
GLOBAL, ID: 0
Forward Mode: redundance Forwarding: On

route-map rm
```

```
route-map index: sequence 10, permit Match rule:
```

```
ACL ID :      0, ACL CLS: 0, Nam
```

Field	Description
Pbr VRF	VRF name and VRF ID.
Forward Mode	Sets the load balance mode or the redundancy mode for the next hop.
Forwarding	Displays whether the IP route forwarding is enabled.
Route-map index	The serial number and the type of the sub-map.
Match rule	Match rule.
Set rule	Set rule.
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.14. show ip pbr source-route

Use this command to display information about IPv4 source address-based PBR.

```
show ip pbr source-route [ interface if-name ]
```

Parameter Description

Parameter	Description
interface <i>if-name</i>	Displays the IPv4 PBR applied to a specified interface if <i>if-name</i> is specified. Displays all applied IPv4 PBR information if <i>if-name</i> is not specified.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

You can use this command to display the configured source address-based PBR.

Configuration Examples

```
QTECH# show ip pbr source-route
PBR IPv4 Source Route
Interface : GigabitEthernet 0/1
Sequence : 10
```

The following example displays information about the configured source address-based PBR.

```
Source address : 10.1.1.1/24
VRF ID : 0
Route Flags :
Route Type : PBR
Direct : Permit
Priority : High
Match_ipaddr : Exist
Mode : redundance
Nexthop Count : 1
Nexthop[0].... 192.168.8.100
Weight[0]      : 1
Ifindex[0]     : 2
```

Field description:

Field	Description
Interface	Interface to which the PBR is applied
Sequence	Sequence number of the PBR
VRF ID	ID of the VRF table associated with an interface
Route Flags	<p>Flag bit of PBR:</p> <p>Route Type: type of routes. The value PBR indicates PBR routes while the value Normal indicates common routes.</p> <p>Direct: PBR matching mode. The options include permit and deny.</p> <p>Priority: priority of a PBR route. The options include High and Low.</p>
Mode	Sets the next hop to work in redundancy mode or load balancing mode.
Nexthop Count	Sets the number of next hops. ECMP supports a maximum of 32 next hops.
Nexthop	Sets the next-hop IPv4 address.
Weight	Sets the next-hop weight value.
Ifindex	Sets the outbound interface index of the next hop.

6.15. show ip pbr statistics

Use this command to display the IPv4 PBR forwarded packet count.

show ip pbr statistics [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv4 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv4 PBR forwarded packet count of all interfaces where the IPv4 PBR is enabled is displayed.
local	Displays the IPv4 PBR forwarded packet count on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the IPv4 PBR forwarded packet count.

```
QTECH#show ip pbr statistics IPv4 Policy-based route statistic gigabitEthernet 0/1
statistics : 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.16. show ip policy

Parameter Description

Use this command to display the interface configured with the policy-based routing and the name of route map applied on the interface.

show ip policy [*route-map-name*]

Parameter	Description
<i>route-map-name</i>	Indicates the name of a route map.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

You can use this command to verify the current PBR configured in the system.

Configuration

The following example displays the current PBR configured in the system.

Examples

```
QTECH#show ip policy Banlance Mode: redundance Interface    Route map
local test
FastEthernet 0/0      test
```

Related Commands

Command	Description
ip policy route-map	Applies the policy-based routing on the

	interface.
ip local policy route-map	Applies the policy-based routing on the local interface.

Platform Description

N/A

6.17. show ipv6 pbr bfd

Use this command to display the correlation between the IPv6 policy router and BFD.

show ipv6 pbr bfd

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```
QTECH# show ipv6 pbr bfd
VRF ID Ifindex Host
```

The following example displays the correlation between the IPv6 policy router and BFD.

```
QTECH# show ipv6 pbr bfd
VRF ID Ifindex Host                               State Refcnt
0      13 2000::2 Up                               1
```

Field Description

Field	Description
VRF ID	VRF of BFD neighbors correlated with the policy router
Ifindex	The interface index of BFD neighbors correlated with the policy router
Host	The peer IPv6 address
State	Up/Down status of BFD neighbors correlated with the policy router
RefCount	Calculation referred by BFD neighbors

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

```
QTECH# show ipv6 pbr bfd
VRF ID Ifindex Host          State Refcnt
    13  2000::2  Up           1
```

6.18. show ipv6 pbr route

Use this command to display the IPv6 PBR information on the interface.

show ipv6 pbr route [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv6 PBR information of this interface is displayed. Otherwise, the IPv6 PBR information of all interfaces where the IPv6 PBR is enabled is displayed.
local	Displays the IPv6 PBR information on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```

QTECH#show ipv6 pbr route PBR IPv6 Route Summary : 1
Interface      : GigabitEthernet 0/2 Sequence      : 10
ACL[0] : 2901
ACL_CLS[0]    : 0
Min Length    : None
Max Length    : None
VRF ID : 0
Route Flags   :

Route Type : PBR Direct : Permit
Priority : High
Tos_Dscp : None Precedence : None Tos_Dscp : 0
Precedence : 0
Mode : redundance Nexthop Count : 1 Nexthop[0] : 10::1
Weight[0] : 1
Ifindex[0] : 3

```

The following example displays the IPv6 PBR information on the interfaces.

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
Min Length	The minimum match length.
Max Length	The maximum match length.
VRF ID	Port associated VRF ID.
Route Flags	<p>PBR flag bit:</p> <p>Route Type: “PBR” indicates PBR routes. “Normal” indicates common routes.</p> <p>Direct: PBR matching action, permit or deny</p> <p>Priority: PBR priority, High or Low</p> <p>Tos_Dscp: Displays whether the tos rule or the dscp rule is configured.</p> <p>Precedence: Displays whether the set ip precedence rule is configured.</p>
Mode	Specifies the redundancy mode or the load balance mode for the next hop.
Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
Nexthop	Specifies the next hop IP address.
Weight	Specifies the next hop weight.
Ifindex	Specifies the outbound interface index corresponding to the next hop

Related Commands

Command	Description
---------	-------------

N/A	N/A
-----	-----

Platform Description

N/A

6.19. show ipv6 pbr route-map

Use this command to display the IPv6 PBR route-map information.

show ipv6 pbr route-map *route-map-name*

Parameter Description

Parameter	Description
<i>route-map-name</i>	The route-map name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```
QTECH#show ipv6 pbr route-map rm6 Pbr VRF: GLOBAL, ID: 0
Forward Mode: redundance Forwarding: On

route-map rm6
route-map index: sequence 10, permit Match rule:
ACL ID :      0, ACL CLS: 0, Name: acl6
Set rule:
IPv6 Nexthop: 10::1, (VRF Name: , ID: 0), Weight: 0, Flags: 0
PBR state info ifx: GigabitEthernet 0/0, Connected: true, Track State: valid, Flags: 0
```

The following example displays the IPv6 PBR route-map information.

Field	Description
Pbr VRF	VRF name and VRF ID.
Forward Mode	Sets the load balancing mode or to the redundancy mode for the next hop.
Forwarding	Displays whether the IP route forwarding is enabled.
Route-map index	The serial number and the type of the sub-map.
Match rule	Match rule
Set rule	Set rule.
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.20. show ipv6 pbr source- route

Use this command to display the IPv6 source address PBR configuration.

show ipv6 pbr source-route [interface *if-name*]

Parameter Description

Parameter	Description
-----------	-------------

interface <i>if-name</i>	<p>(Optional) Displays the IPv6 source address PBR configuration on the specified interface.</p> <p>If the parameter is not configured, the IPv6 source address PBR configuration on all interfaces will be displayed.</p>
---------------------------------	--

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the IPv6 source address PBR configuration.

```
QTECH# show ipv6 pbr source-route PBR IPv6 Source Route
Interface : GigabitEthernet 0/1
Sequence : 10
Source address : 1000::1/64
VRF ID : 0
Route Flags :
Route Type : PBR
Direct : Permit
Priority : High
Match_ipaddr : Exist
Mode : redundance

Nexthop Count : 1
Nexthop[0] : 1001::2
Weight[0] : 1
Ifindex[0] : 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.21. show ipv6 pbr statistics

Use this command to display the IPv6 PBR forwarded packet count.

show ip pbr statistics [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv6 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv6 PBR forwarded packet count of all interfaces where the IPv6 PBR is enabled is displayed.
local	Displays the IPv6 PBR forwarded packet count on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```
QTECH#show ipv6 pbr statistics IPv6 Policy-based route statistic gigabitEthernet 0/1
statistics : 20
```

The following example displays the IPv6 PBR forwarded packet count.

Related Commands

Command	Description
N/A	N/A

Platform Description

6.22. show ipv6 policy

Parameter Description

Use this command to display which interfaces are configured with IPv6 PBR.

show ipv6 policy [*route-map-name*]

Parameter	Description
<i>route-map-name</i>	Name of the PBR router map.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```
QTECH#show ipv6 policy Banlance Mode: redundance
Interface      Route map
VLAN 1 RM_for_Vlan_1
VLAN 2 RM_for_Vlan_2
```

The following example displays the current PBR applied in the system.

Field	Description
Balance Mode	The current PBR running mode.
Interface	The name of interface with PBR applied.
Route map	The name of route map applied on the interface.

Related Commands

Command	Description
show route-map	Displays the current configured route map.

Platform Description

N/A

7. VRF COMMANDS

7.1. address-family

Use this command to configure an IPv4 address family or IPv6 address family for a multiprotocol VRF.

address-family { ipv4 | ipv6 }

Parameter Description

Parameter	Description
ipv4	Enters IPv4 address family.
ipv6	Enters IPv6 address family.

Defaults

No IPv4 address family or IPv6 address family is configured for a multiprotocol VRF.

Command mode

VRF configuration mode

Usage Guide

This command is applicable only to the multiprotocol VRF.

Configuration Examples

```
QTECH(config)#vrf definition vrf1 QTECH(config-vrf)#address-family ipv4
QTECH(config-vrf-af)#
```

The following example defines a multiprotocol VRF vrf1 and configures an IPv4 address family.

Related Commands

Command	Description
exit-address-family	Exits the VRF address family configuration mode.
vrf definition	Defines a multiprotocol VRF.

Platform Description

N/A

7.2. description

Use this command to configure the VRF description.

`description string`

Parameter Description

Parameter	Description
<i>string</i>	VRF description character string. The maximum length is 244 characters.

Defaults

No VRF description is configured by default .

Command mode

VRF configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH(config)#ip vrf definition vrf1
QTECH(config-vrf)#description vpn-a
```

The following example defines a single-protocol IPv4 VRF vrf1 and configure the description to vpn-a.

```
QTECH(config)#vrf definition vrf1
QTECH(config-vrf)#description vpn-b
```

The following example defines a multiprotocol VRF vrf2 and configure the description to vpn-b.

Related Commands

Command	Description
ip vrf	Defines a single-protocol IPv4 VRF.
vrf definition	Defines a multiprotocol VRF.

Platform Description

N/A

7.3. exit-address-family

Use this command to exit VRF address family configuration mode.

exit-address-family

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

VRF address family configuration mode

Usage Guide

N/A

Configuration Examples

The following example defines a multiprotocol VRF *vrf1* and configures an IPv4 address family.

```
QTECH(config)#vrf definition vrf1
```

```
QTECH(config-vrf)#address-family ipv4
```

```
QTECH(config-vrf-af)# exit-address-family QTECH(config-vrf)#
```

Related Commands

Command	Description
address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol VRF.
vrf definition	Defines a multiprotocol VRF.

Platform Description

N/A

7.4. ip vrf

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Use this command to create a VRF. Use the **no** form of this command to delete a VRF.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Defaults

No VRF is configured by default.

Command mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# ip vrf redvrf
QTECH(config-vrf)#
```

The following example creates a VRF.

Related Commands

Command	Description
N/A	N/A

7.5. ip vrf forwarding

Use this command to add an interface or sub-interface to a VRF. Use the no form of this command to quit the VRF.

`ip vrf forwarding vrf-name`

`no ip vrf forwarding vrf-name`

Parameter Description

Parameter	Description
<i>vrf-name</i>	Name of the VRF that the interface or sub-interface joins

Defaults

By default, the interface does not belong to any VRF.

Command mode

Interface configuration mode

Usage Guide

You can bind the interface to the uni-protocol IPv4 VRF without the IPv6 enabled on the interface.

On the device supporting the VRF, if the interface is bound to the uni-protocol IPv4 VRF with the IPv6 protocol enabled, the device cannot forward the IPv6 packets received on this interface.

Configuration Examples

Related Commands

Platform Description

The following example adds an interface or sub-interface to a VRF.

```
QTECH(config-if-GigabitEthernet 0/0)# ip vrf forwardingredvrf
```

Command	Description
N/A	N/A

N/A

7.6. ip vrf receive

Use this command to import the host and direct-connected route of one interface into the specified VRF routing table. Use the **no** form of this command to remove the imported host and

direct-connected route from the VRF.

ip vrf receive *vrf-name*

no ip vrf receive *vrf-name*

Parameter	Description
<i>vrf-name</i>	Name of the VRF that the host and direct-connected route imported to.

Defaults

By default, the host and direct-connected route of the interface are not imported to other VRFs

Command mode

Interface configuration mode

Usage Guide

Currently, the **ip vrf receive** command supports the VRF routing based on the PBR. This command is used to import the host with the main and slave addresses and direct-connected route of this interface into the specified VRF routing table. You need to execute this command multiple times to import this host and direct-connected route to multiple VRF routing tables. Unlike the **ip vrf forwarding** command, which does not bind the interface to the VRF and this interface still belongs to the global VRF. Configuring both **ip vrf**

forwarding and **ip vrf receive** on an interface is not allowed. If one has been configured, configuring the other one will prompt an error message.

If **ip vrf forwarding** has been configured, configuring **ip vrf receive** will prompt:

```
% Cannot configure 'ip vrf receive' if interface is under a VRF
```

If **ip vrf receive** has been configured, configuring **ip vrf forwarding** will prompt:

```
% Cannot bind interface to a VRF if it has configed 'ip vrf receive'
```

Configuration Examples

```
QTECH(config)# interface FastEthernet0/1 QTECH(config-if)# ip address 192.168.1.2 255.255.255.0
QTECH(config-if)# ip policy route-map PBR-VRF-SELECTION QTECH(config-if)# ip vrf receive VRF_1
QTECH(config-if)# ip vrf receive VRF_2
QTECH(config-if)# end
```

The following example imports the host and direct-connected route of one interface into the specified VRF routing table.

Related Commands

Command	Description
ip vrf forwarding	Adds the interface to a VRF.
ip vrf	Creates a VRF.
set vrf	Sets the VRF in the routing map configuration mode.

Platform Description

N/A

7.7. maximum routes

Use this command to set the maximum routes limit within the VRF. Use the **no** form of this command to remove the setting.

maximum routes *limit* { *warn-threshold* | **warning-only** }

no maximum routes

Parameter

Description

Parameter	Description
<i>limit</i>	The maximum number of routes, in the range from 1 to 4,294,967,295. The routes which exceed the limits will not be added to the core routing table.
<i>warn-threshold</i>	The warning will be printed when the threshold is reached. The threshold value is in the range from 1 to 100.
warning-only	After the number of routes reaches <i>limit</i> , the warning will be printed but the routes will be added to the core routing table.

Defaults

N/A

Command Mode

Single-protocol VRF is configured in VRF configuration mode; multiple-protocol VRF is configured in address family mode.

Usage Guide

```
QTECH(config)# ip vrf vrf1
QTECH(config-vrf)# maximum routes 1000 warning-only
```

This command is used to set the maximum number of routes for the VRF.

Configuration Examples

The following example sets the maximum number of routes for vrf1 to 1,000, and enables the device to only print the warning.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.8. vrf definition

Use this command to create the multiprotocol VRF.

vrf definition *vrf-name*

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name, no more than 31 characters.

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

The single-protocol VRF configuration command **ip vrf** cannot be used to edit a multiprotocol VRF; the multiprotocol VRF configuration command **vrf definition** cannot be used to edit a single-protocol

IPv4 VRF.

Configuration Examples

```
QTECH(config)#vrf definition vrf1
QTECH(config-vrf)#
```

The following example s creates a multiprotocol VRF *vrf1*.

Related Commands

Command	Description
description	Configures the description.
address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol

	VRF.
exit-address-family	Exits the VRF address family configuration mode.
vrf forwarding	Binds a network interface to a multiprotocol VRF.

Platform Description

N/A

7.9. vrf forwarding

Use this command to bind a network interface to a multiprotocol VRF.

`vrf forwarding vrf-name`

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name, which shall be a multiprotocol VRF instead of a single-protocol VRF that supports IPv4 only.

Defaults

The network interface is not bound to any VRF.

Command mode

Interface configuration mode

Usage Guide

The configuration command **ip vrf forwarding** cannot be used to bind a network interface to a multiprotocol VRF; the configuration command **vrf forwarding** cannot be used to bind a network interface to a single-protocol IPv4 VRF.

An interface cannot be bound to a multiprotocol VRF that is not configured with any address family. To bind a network interface to a multiprotocol VRF, you should delete the existing IPv4 addresses, VRRP IPv4 addresses, IPv6 addresses and VRRP IPv6 addresses, and disable IPv6 on the interface. When a network interface is bound to a multiprotocol VRF, no IPv4 address or VRRP IPv4 address should be configured for the interface if no IPv4

address family is configured for the VRF. You should configure an IPv4 address family for the VRF before configuring an IPv4 address and VRRP IPv4 address for the interface.

When a network interface is bound to a multiprotocol VRF, no IPv6 address or VRRP IPv6 address should be configured for the interface if no IPv6 address family is configured for the VRF. You should configure an IPv6 address family for the VRF before configuring an IPv6 address and VRRP IPv6 address for the interface.

If you delete a multiprotocol VRF's IPv4 address family, you should delete the IPv4 addresses and VRRP IPv4 addresses of all network interfaces bound to the VRF, and delete the IPv4 static routes whose routing VRF or next-hop VRF is that VRF. Likewise, if you delete a multiprotocol VRF's IPv6 address family, you should delete the IPv4 addresses and VRRP IPv6 addresses of all network interfaces bound to the VRF, disable IPv6 on the interfaces, and delete the IPv6 static routes whose routing VRF or next-hop VRF is that VRF.

Configuration Examples

The following example binds the interface VLAN 1 to a multiprotocol VRF vrf1.

```
QTECH(config)#vrf definition vrf1 QTECH(config-vrf)#address-family ipv4 QTECH(config-vrf-af)#exit-address-family QTECH(config-vrf)#address-family ipv6 QTECH(config-vrf-af)#exit-address-family
```

```
QTECH(config-vrf)#interface vlan 1 QTECH(config-if)#vrf forwarding vrf1
QTECH(config-if)#ip address 1.1.1.1 255.255.255.0
QTECH(config-if)#ipv6 address 1000::1/64
```

Related Commands

Command	Description
vrf definition	Defines a multiprotocol VRF.

Platform Description

N/A

7.10. vrf receive

Use this command to add the local host's route and direct route with the interface's IPv4/v6 address to the routing table of the specified VRF.

vrf receive *vrf-name*

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name, which should be a multiprotocol VRF instead of a single-protocol IPv4 VRF.

Defaults

N/A

Command mode

Interface configuration mode

Usage Guide

This command is not used to bind an interface to a VRF, and the interface is still a global interface.

If the administrator needs to use PBR to choose VRF, the **vrf receive** command should be configured on the interfaces where PBR is applied for each selected VRF.

When an IPv4 address family is configured for a multiprotocol VRF, the local host's route and direct route with the interface's IPv4 address is added to the IPv4 routing table of the specified VRF, and the local host's route with the IPv4 address of the master VRRP group on the interface is added to the IPv4 routing table of the specified VRF. When an IPv6 address family is configured for a multiprotocol VRF, the local host's route and direct route with the interface's IPv6 address is added to the IPv6 routing table of the specified VRF, and the local host's route with the IPv6 address of the master VRRP group on the interface is added to the IPv6 routing table of the specified VRF.

The **ip vrf forwarding** and **vrf receive** commands are mutually exclusive on an interface, and so are the **vrf forwarding** and **vrf receive** commands. If both commands are configured on an interface, an error message will be shown.

If the **ip vrf forwarding** or **vrf forwarding** command is configured first, and then the **vrf receive**

command is configured, the following message will be displayed:

% Cannot configure 'vrf receive' if interface is under a VRF If the **vrf receive** command is configured first, and then the **ip vrf forwarding** or **vrf forwarding** command is configured, the following message will be displayed:

```
% Cannot configure 'vrf forwarding vrf2' on this interface, please delete 'ip
vrf receive' and 'vrf receive' first.
```

Configuration Examples

The following example selects a VRF using IPv6 PBR on VLAN 1.

```
QTECH(config)#vrf definition vrf1 QTECH(config-vrf)#address-family ipv6 QTECH(config-vrf-
```

```
af)#exit-address-family
```

```
QTECH(config-vrf)#vrf definition vrf2 QTECH(config-vrf)#address-family ipv6 QTECH(config-vrf-af)#exit-address-family
```

```
QTECH(config-vrf)#route-map pbr-vrf-selection permit 10 QTECH(config-route-map)#match ipv6 address acl1 QTECH(config-route-map)#set vrf vrf1
```

```
QTECH(config-route-map)#route-map pbr-vrf-selection permit 20 QTECH(config-route-map)#set vrf vrf2
```

```
QTECH(config-route-map)#interface vlan 1
```

```
QTECH(config-if)#ipv6 policy route-map pbr-vrf-selection QTECH(config-if)#ipv6 address 1000::1/64
```

```
QTECH(config-if)#vrf receive vrf1
```

```
QTECH(config-if)#vrf receive vrf2
```

Related Commands

Command	Description
vrf definition	Defines a multiprotocol VRF.
address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol VRF.
set vrf	Configures a VRF in the route map configuration mode.

Platform Description

N/A

7.11. show ip vrf

Use this command to display the VRF information.

show ip vrf [brief | detail | interfaces]

Parameter Description

Parameter	Description
brief	(Optional) Displays the VRF information in brief.
detail	(Optional) Displays the VRF information in detail.
interfaces	(Optional) Displays the VRF's interface information in detail.

Defaults

All VRF information is displayed without parameter specified.

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the VRF information, which can be divided into two levels:

Use the keyword **brief** to display the information in brief.

Use the keyword **detail** to display the information in detail.

Use the keyword **interfaces** to display the VRF's interface information.

Configuration Examples

The following example displays the VRF information.

```
QTECH#show ip vrf
```

```

Name                Interfaces
Aaa                  GigabitEthernet 0/0
                     GigabitEthernet 0/1

```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.12. show vrf

Use this command to display the VRF configuration (including the single-protocol VRF and the multiple-protocol VRF).

show vrf [ipv4 | ipv6 | brief | count | detail]

Parameter Description

Parameter	Description
ipv4	Displays the brief VRF (the single-protocol VRF) information of the IPv4 address family.
ipv6	Displays the VRF brief information of the IPv6 address family.
brief	Displays the brief VRF (including the single-protocol VRF and the multiple-protocol) information.
count	Displays the capacity of VRF and its current value.
detail	Displays the detailed VRF (including the single-protocol VRF and the multiple-protocol) information.

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays brief information about all VRF.

7. VRF Commands

```
QTECH#show vrf
```

```

Name      Default RD   Protocols   Interfaces
aaa       <not        set>        ipv4
aab       <not        set>
bbb       <not        set>        ipv6
ccc       <not        set>        ipv4,ipv6   V11

```

:

Field	Description
Name	VRF name.
Default RD	Default RD of the VRF.
Protocol	The address family of the VRF. IPv4 indicates the VRF is enabled in the IPv4 address family mode; ipv6 indicates the VRF is enabled in the IPv6 address family mode.
Interfaces	The interface list of the VRF. The interface where the [ip] vrf forwarding command has been configured will be displayed on that list.

Command	Description
N/A	N/A

N/A

8. RIPNG COMMANDS

8.1. clear ipv6 rip

Use this command to clear the RIPng routes.

```
clear ipv6 rip
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

None

Command mode

Privileged EXEC mode

Usage Guide

Running this command removes all RIPng routes and this operation may have great impact on the RIPng protocol. This command should be used with caution.

Configuration Examples

Related Commands

Platform Description

The following example clears the RIPng routes:

```
QTECH# clear ipv6 rip
```

Command	Description
---------	-------------

N/A	N/A
-----	-----

N/A

8.2. default-metric

Use this command to configure the default metric for RIPng. Use the **no** form of this command to restore the default value.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
<i>metric</i>	Sets the default metric value. The valid range is from 1 to 16. The route is unreachable if the metric value is larger than or equal to 16.

Defaults

The default value is 1.

Command mode

Routing process configuration mode.

Usage Guide

This command shall be used with the **redistribute** command. When redistributing the route from one route process to RIPng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPng metric value shall be defined when translating the metric values. If there is no defined metric value, use the **default-metric** command to define one; and the defined metric value will overwrite the value of the **default-metric** command. By default, the **default-metric** value is 1.

Configuration Examples

The following example shows how to set the RIPng metric value as 3 when redistributing OSPF process 100:

```
QTECH(config-router)# default-metric 3
QTECH(config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the route from one route domain to another route domain.

Platform Description

N/A

8.3. distance

Use this command to set the administrative distance of RIPng. Use the no form of this command to restore the default value.

distance distance

no distance

Parameter Description

Parameter	Description
<i>distance</i>	Sets the RIPng administrative distance. The range is from 1 to 254.

Defaults

The default distance is 120

Command mode

Routing process configuration mode.

Usage Guide

N/A

Configuration Examples

The following example shows how to set the RIPng administrative distance as 160:

```
QTECH(config)# ipv6 router rip
```

Related Commands

Platform Description

```
QTECH(config-router)# distance 160
```

Command	Description
N/A	N/A

N/A

8.4. distribute-list

Use this command to filter the in/out route in the prefix list. Use the no form of this command to remove route filtering.

```
distribute-list prefix-list prefix-list-name { in | out } [ interface-type interface-name ]
```

```
no distribute-list prefix-list prefix-list-name { in | out } [ interface-type interface-name ]
```

Parameter Description

Parameter	Description
prefix-list <i>prefix-list-name</i>	Name of the prefix list which is used to filter the route.
in out	Filters the in or out route in the distribute list.
<i>interface-type</i> <i>interface-name</i>	(Optional) Applies the distribute list to the specified interface.

Defaults

By default, no distribute list is defined.

Command mode

Routing process configuration mode.

Usage Guide

This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.

Configuration Examples

The following example shows how to filter the received update route on the interface eth0 (only those update routes within the **prefix-list allowpre** prefix list range can be received)

```
QTECH(config)# ipv6 router rip
QTECH(config-router)# distribute-list prefix-list allowpre in eth0
```

Related Commands

Command	Description
redistribute	Sets route redistribution.

Platform Description

N/A

8.5. graceful-restart

Use this command to configure the graceful restart (GR) function for the RIPng process.

graceful-restart [**grace-period** *grace-period*]

Use the **no** form of this command restore the default configurations.

no graceful-restart [*grace-period*]

Parameter Description

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	Displays the configured grace period.

<i>grace-period</i>	<p>Indicates the configured GR period, ranging from 1 to 1800 seconds.</p> <p>The default value is the smaller between twice of the update time and 60s.</p>
---------------------	--

Defaults

The GR function is enabled by default.

Command Mode

Routing process configuration mode

Default Level

14

Usage Guide

The GR function is configured based on RIPng instances. Different parameters can be configured for different RIPng instances as required.

The GR period indicates the maximum duration from RIPng restart to RIPng GR completion. In this time period, the forwarding table before restart is used and the RIPng route is restored to the status before restart. After the GR period expires, the RIPng process exits the GR status and the common RIPng operation is performed.

The graceful-restart grace-period command allows a user to modify the GR period in explicit mode. Note that GR is completed and the RIPng route is updated once before the RIPng route becomes invalid. If the GR period is improperly set, continuous data forwarding in the GR process cannot be ensured. A typical case is as follows:

If the GR period is greater than the invalid time of the neighbor route, GR is not completed before the route becomes invalid and the route is not advertised to the neighbor again. The neighbor route stops forwarding data after the route becomes invalid, resulting in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the GR period needs to be configured, check configuration of the timers command to ensure that the GR period value is greater than the route update time and smaller than the route invalid time.

When GR is performed for the RIPng process, ensure that the network environment is stable.

Configuration Examples

```
QTECH(config)# ipv6 router rip
QTECH(config-router)# graceful-restart grace-period 90
```

The following example enables the GR function for the RIPng process and configures the GR period.

Verification

Run the **show ipv6 rip** command to check whether the GR function is configured and query the configured grace period.

Prompts

N/A

Common Errors

N/A

Platform Description

N/A

8.6. ipv6 rip default-information

Use this command to generate a default IPv6 route to the RIPng. Use the **no** form of this command to remove the default route.

ipv6 rip default-information { **only** | **originate** } [**metric** *metric-value*]

no ipv6 rip default-information

Parameter Description

Parameter	Description
only	Advertises the IPv6 default route only.
originate	Advertises both of the IPv6 default route and other routes.
metric <i>metric-value</i>	Sets the metric value for the default route. The valid range is from 1 to 15. The default metric is 1.

Defaults

By default, no default route is configured.

Command mode

Interface configuration mode

Usage Guide

With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPng route database.

To avoid the route loop, once this command has been configured on the interface, RIPng refuses to receive the default route update message advertised from the neighbor.

Configuration Examples

```
QTECH(config)# interface ethernet 0/0
QTECH(config-if)# ipv6 rip default-information only
```

The following example shows how to create a default route to the RIPng routing process on the interface ethernet0/0 and enable this interface to advertise the default route only:

Related Commands

Command	Description
show ipv6 rip	Displays the RIPng process and statistics.
show ipv6 rip database	Displays the RIPng route.

Platform Description

N/A

8.7. ipv6 rip enable

Use this command to enable the RIPng on the interface. Use the **no** form of this command to disable RIPng on the interface.

ipv6 rip enable

no ipv6 rip enable

Parameter Description

Parameter	Description
-----------	-------------

N/A	N/A
-----	-----

Defaults

It is disabled by default.

Command mode

Interface configuration mode.

Usage Guide

This command is used to add the RIPng interface. Before this command is configured, if the RIPng is not enabled, use this command to enable the RIPng automatically.

Configuration Examples

The following example shows how to enable the RIPng on the interface 0/0:

```
QTECH(config)# interface ethernet 0/0
QTECH(config-if)# ipv6 rip enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.8. ipv6 rip metric-offset

Use this command to set the interface metric value. Use the **no** form of this command to remove the metric configurations.

ipv6 rip metric-offset **value**

no ipv6 rip metric-offset

Parameter Description

Parameter	Description
<i>value</i>	Sets the interface metric value on the interface. The valid range is from 1 to 16.

Defaults

The default value is 1.

Command mode

Interface configuration mode.

Usage Guide

Before the route is added to the routing list, the interface metric value shall be upon the route metric.

To this end, the interface metric value influences the route usage.

```
QTECH(config)# interface ethernet 0/1
QTECH(config-if)# ipv6 rip metric-offset 5
```

Configuration Examples

The following example shows how to set the metric value of the interface Ethernet 0/1 as 5:

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.9. ipv6 rip subvlan

Use this command to enable RIPng on super VLANs. Use the **no** form of this command to restore the default setting.

Ipv6 rip subvlan [all | **vid**] no ipv6 rip subvlan

Parameter Description

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults

The default setting takes effect only on super VLANs with RIPng disabled.

Command Mode

Interface configuration mode.

Usage Guide

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIPng multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIPng multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the RIPng function does not need to be enabled on a super VLAN. Therefore, the RIPng function is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration Examples

The following example sends the RIPng multicast packets to sub VLAN 1024 of super VLAN 300.

```
QTECH(config)# interface vlan 300
QTECH(config-if-VLAN 300)# ipv6 rip subvlan 1024
```

8.10. ipv6 router rip

Use this command to create the RIPng process and enter routing process configuration mode. Use the **no** form of this command to remove the RIPng process.

ipv6 router rip

no ipv6 router rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No RIPng process is configured by default.

Command mode

Global configuration mode.

Usage Guide N/A.

Configuration Examples

Related Commands

The following example shows how to create the RIPng process and enter routing process configuration mode:

```
QTECH(config)# ipv6 router rip
```

Command	Description
ipv6 rip enable	Enables the RIPng on the specified interface.

Platform Description

N/A

8.11. passive-interface

Use this command to disable the interface to send update packets. Use the **no** form of this command to enable the interface to send update packets.

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description

Parameter	Description
default	Enables the passive mode on all interfaces.
<i>interface-type</i> <i>interface-num</i>	Interface type and interface number.

Defaults

No passive interface is configured by default.

Command mode

Routing process configuration mode.

Usage Guide You can use the **passive-interface default** command to enable the passive mode on all interfaces. Then ,use the **no passive-interface** *interface-type interface-num* command to remove the specified interface from the passive mode.

Configuration Examples

The following example shows how to enable the passive mode on all interfaces and remove interface ethernet 0/0 from the passive mode:

```
QTECH(config-router)# passive-interface default
QTECH(config-router)# no passive-interface ethernet 0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.12. redistribute

Use this command to redistribute the route of other routing protocols to RIPng. Use the **no** form of this command to remove the redistribution configuration.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value*]

route-map *route-map-name*]

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value*]

route-map *route-map-name*]

Parameter Description

Parameter	Description
bgp	Redistributes the BGP routes to RIPng.
connected	Redistributes the connected routes to RIPng.
isis [<i>area-tag</i>]	Redistributes the ISIS routes to RIPng. <i>area-tag</i> indicates the ISIS process number.
ospf <i>process-id</i>	Redistributes the OSPF routes to RIPng. <i>process-id</i> indicates the OSPF process number, and the range is from 1 to 65,535.
static	Redistributes the static routes to RIPng.
metric <i>metric-value</i>	(Optional) Sets the metric value for the route redistributed to RIPng.
route-map <i>route-map-name</i>	(Optional) Sets the redistribution route filtering.

Defaults

By default, the routes of other routing protocols are not redistributed.

If the **default-metric** command is not configured, the default metric value is 1; By default, the **route-map** is not configured;

By default, all sub-type routes in the specified routing process are redistributed.

Command mode

Routing process configuration mode.

Usage Guide

This command is used to redistribute the external routes to RIPng.

It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different. The RIP and OSPF metric calculations are incomparable for the reason that the RIP metric calculation is hop-based while the OSPF one is bandwidth-based.

The instance, from where the routing information is redistributed to the RIPng, must be specified in the process of configuring the multi-instance protocol redistribution.

Configuration Examples

```
QTECH(config)# ipv6 router rip
QTECH(config-router)# redistribute static route-map
```

The following example shows how to redistribute the static route, use the route map *mymap* to filter and set the metric value as 8:

Related Commands

Command	Description
default-metric	Defines the default RIPng metric value when redistributing other routing protocols.
distribute-list	Filters the RIPng routing update packets.

Platform

N/A

Description

8.13. show ipv6 rip

Use this command to show the parameters and each statistical information of the RIPng routing protocol process.

```
show ipv6 rip
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode or user mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show ipv6 rip Routing Protocol is "RIPng"
Sending updates every 10 seconds with +/-50%, next due in 8 seconds Timeout after 30
seconds, garbage collect after 60 seconds
Outgoing update filter list for all interface is: distribute-list prefix aa out
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and each statistical information of the RIPng process.

Platform Description

N/A

8.14. show ipv6 rip database

Use this command to display the RIPng route entries.

show ipv6 rip database

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode or user mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show ipv6 rip database
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP sub-codes:n - normal,s -
static,d - default,r - redistribute, i - interface, a/s - aggregated/suppressed
S(r) 2001:db8:1::/64, metric 1, tag 0 Loopback 0/::
S(r) 2001:db8:2::/64, metric 1, tag 0 Loopback 0/::
C(r) 2001:db8:3::/64, metric 1, tag 0 VLAN 1/::
S(r) 2001:db8:4::/64, metric 1, tag 0 Null 0/::
C(i) 2001:db8:5::/64, metric 1, tag 0 Loopback 1/::
S(r) 2001:db8:6::/64, metric 1, tag 0
Null 0/::
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.15. split-horizon

Use the **split-horizon** command to enable the RIPng split-horizon function in routing process configuration mode. Use the **no** form of this command to disable this function. Use the **split-horizon poisoned-reverse** command to enable the RIPng poisoned reverse horizontal split function in routing process configuration mode. Use the **no** form of this command to disable this function.

split-horizon [**poisoned-reverse**]

no split-horizon [**poisoned-reverse**]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables the poisoned-reverse horizontal split.

Defaults

RIPng split horizon is enabled by default.

Command mode

Routing process configuration mode.

Usage Guide

In the process of packet updating, split-horizon function prevents some routing information from being advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the **show ipv6 rip** command to determine whether the RIPng split-horizon function is enabled or not.

Configuration Examples

The following example shows how to disable the RIPng horizontal split:

```
QTECH(config)# ipv6 router rip
QTECH(config-router)# no split-horizon
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.16. timers

Use this command to adjust the RIPng timer. Use the no form of this command to restore the default settings.

timers update invalid flush

no timers

Parameter Description

Parameter	Description
<i>update</i>	Sets the routing update time, in seconds. The update parameter defines the period of sending the routing update packets by the device. The invalid and flush parameter reset once the update packets are received.
<i>invalid</i>	Sets the routing invalid time, in seconds, starting from receiving the last valid update packet. The invalid parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
<i>flush</i>	Sets the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.

Defaults

The default update time is 30 seconds; the default invalid time is 180 seconds; and the default flush time is 120 seconds.

Command mode

Routing process configuration mode.

Usage Guide

Adjusting the above time may speed up the RIPng convergence time and the troubleshooting time. The RIPng time must be consistent for the devices connecting to the same network. You are not recommended to adjust the RIP time, except for the specific requirement.

Use the **show ipv6 rip** command to view the current RIPng time parameter setting.

In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.

Configuration Examples

The following example shows how to send the RIP update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds.

```
QTECH(config)# ipv6 router rip
QTECH(config-router)# timers 10 30 90
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and the statistical information of the RIPng process.
show ipv6 rip database	Displays the RIPng routes.

Platform Description

N/A

9. NSM COMMANDS

9.1. clear ip route

Use this command to clear the route cache.

clear ip route [*vrf vrf_name*] { * | *network* [*netmask*] | }

Parameter	Description
<i>vrf vrf_name</i>	(Optional) Specifies the route cache of the specified VRF instance. If no VRF is specified, the route cache of all VRF instances is cleared.
*	Clears all route cache.
<i>network</i>	Specifies the route cache of the network or subnet.
<i>netmask</i>	(Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match <i>network</i> with the route. The cache of the longest match is cleared.

Parameter Description

Command Mode

Privileged EXEC mode

Usage Guide

Clearing route cache clears the corresponding routes and triggers the routing protocol relearning. Please note that clearing all route cache leads to temporary network disconnection.

Examples

Related Commands

The following example clears the cache of the route which is the longest

match with IP address 192.168.12.0.

clear ip route 192.168.12.0

Command	Description
N/A	N/A

Platform Description

This command is not supported on 2-layer devices.

9.2. ip default-network

Use this command to configure the default network globally. Use the **no** or **default** form of this command to restore the default setting.

ip default-network *network*

no ip default-network *network*

default ip default-network *network*

Parameter Description

Parameter	Description
<i>network</i>	Default network

Defaults

The default is 0.0.0.0/0.

Command Mode

Global configuration mode

Usage Guide

The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network.

The default network always starts with an asterisk ("*"), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.

Examples


```
ip route 192.168.100.0 255.255.255.0 serial 0/1
ip default-network 192.168.100.0
```

Related Commands

Command	Description
show ip route	Displays the routing table.

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
ip default-network 200.200.200.0
```

9.3. ip fast-reroute route-map

Use this command to enable static fast reroute. Use the **no** or **default** form of this command to restore the default setting.

ip fast-reroute [**vrf** *vrf-name*] **static route-map** *route-map-name*

no ip fast-reroute [**vrf** *vrf-name*]

default ip fast-reroute [**vrf** *vrf-name*] **route-map**

Parameter Description

Parameter	Description
vrf <i>vrf-name</i>	VRF
route-map <i>route-map-name</i>	Route map
static	Backup route

Default

This function is disabled by default.

Command Mode

Global configuration mode

Usage guideline

Fast reroute provides an active next-hop and a backup one. If the active next-hop fails, the backup next-hop is used for forwarding.

To enhance the performance of fast reroute, enable the BFD detection function for the active next-hop.

For interfaces that are up or down, to shorten the interruption time of fast reroute, configure **carrier-delay 0** in the interface configuration mode of the active outbound interface to optimize the performance.

For static fast reroute, if the active next-hop fails, the backup next-hop is used for forwarding.

Examples

The following example sets the backup next-hop of all static routes to 192.168.1.2 through the outbound interface of GigabitEthernet 0/1.

```
QTECH(config)# route-map fast-reroute
QTECH(config-route-map)# set fast-reroute backup-nexthop GigabitEthernet 0/1 192.168.1.2
QTECH(config-route-map)# exit
QTECH(config)# ip fast-reroute static route-map fast-reroute
```

Related command

Command	Description
fast-reroute	Configures OSPF fast reroute.

Platform Description

This command is not supported on 2-layer devices.

9.4. ip route

Use this command to configure a static route. Use the no or default form of this command to restore the default setting.

```
ip route [ vrf vrf_name ] network net-mask { ip-address | interface [ ip-address ] } [ distance ]
[ tag tag ] [ permanent | {track object-number | arp} ] [ weight number ] [description
description-text] [ disabled
```

```
| enabled] [ global ]
```

```
no ip route [ vrf vrf_name ] network net-mask { ip-address | interface [ ip-address ] }
[ distance ]
```

```
no ip route [ vrf vrf_name ] all
```

```
default ip route [ vrf vrf_name ] network net-mask { ip-address | interface [ ip-address ] }
[ distance ]
```

```
default ip route [ vrf vrf_name ] all
```

Parameter	Description
-----------	-------------

vrf <i>vrf_name</i>	Name of the VRF, which can be the single protocol IPv4 VRF or configured IPv4 address family multi-protocol VRF.
<i>network</i>	Network address of the destination
<i>net-mask</i>	Mask of the destination
<i>ip-address</i>	The next hop IP address of the static route
<i>interface</i>	(Optional) The next hop egress of the static route
<i>distance</i>	(Optional) The administrative distance of the static route
<i>tag</i>	(Optional) The tag of the static route
<i>permanent</i>	(Optional) Permanent route ID
<i>track object-number</i>	(Optional) Indicates correlation with Track. object-number indicates the ID of the track object. By default, the static route is not correlated with the Track function.
<i>weight number</i>	(Optional) Indicates the weight of the static route. The weight is 1 by default.
<i>description description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. description-text is a string of one to 60 characters.
<i>disabled/enabled</i>	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
<i>global</i>	(Optional) Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by vrf name.

Parameter Description

Defaults

No static route is configured by default.

Command Mode

Global configuration mode

Usage Guide

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

You can specify the VRF that the static route belongs to. The default weight of the static route is 1. To view the static route of non default weight, execute the `show ip route weight` command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries. WCMP limit is generally 32 for routers. However, WCMP limit varies by switch models for their chipsets support different weights. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it. Association between a static route and an ARP object can be specified. When association between a static route and an ARP object is configured and the ARP object corresponding to the next hop and egress of the route does not exist, the static route does not take effect. When the ARP object corresponding to the next hop and egress of the route exists, the static route takes effect based on another status. Association between a static route and an ARP object cannot be used for routes with the permanent attribute.

hop is 192.168.12.1 and administrative distance is 15.

```
ip route 172.16.199.0 255.255.255.0 192.168.12.1 155
```

If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures data flows to be sent through fastethernet 0/0 to the destination network of 172.16.100.0/24.

```
ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1
```

Related Commands

This command is not supported on 2-layer devices.

9.5. ip route static bfd

Use this command to correlate the static route with BFD. Use the **no** or **default** form of this command to restore the default setting.

ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*] **no ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*] **default ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

Use this command to correlate the static route with BFD. Use the **no** or **default** form of this command to restore the default setting.

Parameter	Description
vrf <i>vrf-name</i>	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
<i>interface-type interface-number</i>	Interface type and interface number.
<i>gateway</i>	Specifies the gateway IP address, that is, the BFD neighbor IP address. If the next hop of the static route is the neighbor, the BFD will detect whether this neighbor is reachable.
source <i>ip-address</i>	(Optional) The source IP address of the BFD session. If the neighbor device is multi hops away, you should specify the source IP address for the BFD session. No source IP address is specified by default.

Parameter Description

Defaults

The static address is not correlated with BFD by default.

Command Mode

Global configuration mode

Usage Guide

Please make sure the BFD session parameters have been configured before executing this command. neighbor 172.16.0.2.

```
QTECH(config)# interface GigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)# no switchport // No need to perform this command on
the router.
QTECH(config-if-GigabitEthernet 0/1)# ip address 172.16.0.1 255.255.255.0 QTECH(config-
if-GigabitEthernet 0/1)# bfd interval 50 min_rx 50 multiplier 3
QTECH(config-if-GigabitEthernet 0/1)#exit
QTECH(config)# ip route static bfd GigabitEthernet 0/1 172.16.0.2 QTECH(config)# ip route
10.0.0.0 255.0.0.0 GigabitEthernet 0/1 172.16.0.2
```

Related Commands

N/A

Platform Description

This command is not supported on 2-layer devices.

9.6. ip route static inter-vrf

Use this command to enable packets to be forwarded over VRF instances through the static route. Use the **no** or **default** form of this command to disable this function.

ip route static inter-vrf no ip route static inter-vrf

default ip route static inter-vrf

Use this command to enable packets to be forwarded over VRF instances through the static route. Use the **no** or **default** form of this command to disable this function.

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

```
*Aug 7 10:58:34: %NSM-6-ROUTESACROSSVRF: Un-installing route [x.x.x.x/8] from  
global routing table with outgoing interface x/x.
```

If the **no** form of this command is executed, packets are unable to be forwarded over VRF instances through the static route. If this command is executed and you want to use the **no** form of this command to disable such function, the following information will be displayed.

Examples

The following example disables packets to be forwarded over VRF instances through the static route.

```
QTECH(config)# no ip route static inter-vrf
```

Related Commands

N/A

Platform Description

This command is not supported on 2-layer devices.

9.7. ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** or **default** form of this command to disable this function.

ip routing no ip routing

default ip routing

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

IP routing is not necessary when the switch serves as bridge or VoIP gateway.

When a device functions only as a bridge or VoIP gateway, the IP routing function of the software is not required. In this case, the IP routing function of the software can be disabled. After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the **no ip routing** command, the

configuration of a large number of static routes may be lost. To prevent this situation, the static route configuration will be hidden temporarily when the **no ip routing** command is run. If the **ip routing** command is run again, the static route configuration can be restored.

Note that if the process or whole system restarts when the **no ip routing** command is run, the static route configuration will not be reserved.

Examples

The following example disables IP routing.

```
QTECH(config)# no ip routing
```

Related Commands

N/A

Platform Description

This command is not supported on 2-layer devices.

9.8. ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

ip static route-limit *number* no ip static route-limit default ip static route-limit

Parameter Description

Parameter	Description
<i>number</i>	Upper threshold of static routes in the range from 1 to 10000

Defaults

The default is 1000.

Command Mode

Global configuration mode

Usage Guide

The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running-config** command.

The following example sets the upper threshold of the static routes to 9000 and then restores the setting to the default value.

Examples

Related Commands

N/A

Platform Description

This command is not supported on 2-layer devices.

9.9. ipv6 route

Use this command to configure an ipv6 static route. Use the no or default form of this command to restore the default setting.

```
ipv6 route [ vrf vrf-name ] ipv6-prefix / prefix-length { ipv6-address [ nexthop-vrf { vrf-name1 / default } ] | interface [ ipv6-address [ nexthop-vrf { vrf-name1 / default } ] ] } [ distance ] [ tag tag ] [ weight number ] [description description-text]
```

```
no ipv6 route [ vrf vrf-name ] ipv6-prefix / prefix-length { ipv6-address [ nexthop-vrf { vrf-name1 / default } ] | interface [ ipv6-address [ nexthop-vrf { vrf-name1 / default } ] ] } [ distance ]
```

Parameter Description

Parameter	Description
vrf vrf-name	Name of VRF, which must be the configured IPv6 address family multi-protocol VRF
prefix-length	Mask length of the destination
ipv6-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
nexthop-vrf vrf-name1	(Optional) VRF the nexthop belongs, which must be the configured IPv6 address family multi-protocol VRF.
distance	(Optional) The administrative distance of the static route.

	The default is 1.
<i>tag</i>	(Optional) The tag value of the static route. The default is 0.
weight <i>number</i>	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
description <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of one to 60 characters.

no ipv6 route [vrf vrf_name] all

default ipv6 route [vrf vrf-name] ipv6-prefix / prefix-length { ipv6-address [nexthop-vrf { vrf-name1 |

default }] | interface [ipv6-address [nexthop-vrf { vrf-name1 | default }]] [distance]

default ipv6 route [vrf vrf_name] all

Defaults

No IPv6 static route is configured by default.

Command Mode

Global configuration mode

Usage Guide

When the multi-protocol VRF deletes the IPv6 address family, the IPv6 static route of VRF that the route or nexthop belongs is deleted.

If the VRF of the IPv6 static route interface is not same as the nexthop's VRF, then this IPv6 static route takes no effect.

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

Examples

Related Commands

Command	Description
show ipv6 route	Displays IPv6 routing table.

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115.

```
ipv6 route 2001::/64 2002::2 115
```

If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures that data flows are sent through fastethernet 0/0 to the destination network of 2001::/64.

```
ipv6 route 2001::/64 fastethernet 0/0 2002::2
```

Platform Description

This command is not supported on 2-layer devices.

9.10. ipv6 route static bfd

Use this command to correlate the static route with BFD. Use the **no** or **default** form of this command to restore the default setting.

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

no ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

default ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

Parameter Description

Parameter	Description
vrf <i>vrf-name</i>	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
<i>interface-type interface-number</i>	Interface type and interface number.
<i>gateway</i>	Specifies the gateway IP address, that is, the BFD neighbor IP address. If the next hop of the static route is the neighbor, the BFD will detect whether this neighbor is reachable.
source <i>ipv6-address</i>	(Optional) The source IP address of the BFD session. If the neighbor device is multi hops away, you should specify the source IP address for the BFD session. No source IP address is specified by default.

Defaults

The static route is not associated with BFD by default.

Command Mode

Global configuration mode

Usage Guide Please make sure the BFD session parameters have been configured before executing this command.

The following example correlates the static route with BFD, and detects the reachability of path to the neighbor *2001:1::2*.

Examples

```
QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if)# no switchport //
QTECH(config-if)# ip address 2001:1::1/64
```

```
QTECH(config-if)# bfd interval 50 min_rx 50 multiplier 3 QTECH(config-if)#exit
QTECH(config)# ipv6 route static bfd GigabitEthernet 0/1 2001:1::2
QTECH(config)# ipv6 route 2002::/64 GigabitEthernet 0/1 2001:1::2
```

Related

Commands N/A

Platform Description

This command is not supported on 2-layer devices.

9.11. ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

Ipv6 static route-limit **number** no ipv6 static route-limit default ipv6 static route-limit

Parameter Description

Parameter	Description
<i>number</i>	Upper threshold of static routes in the range from 1 to 10000.

Defaults

The default is 1000.

Command Mode

Global configuration mode

Usage Guide

The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.

Examples

The following example sets the upper threshold of global ipv6 static routes to 900, default VRF static routes to 200, VRF test static routes to 100, and then restores the setting to the default value.

```
QTECH(config)#ipv6 static route-limit ?  
  <1-10000> Global limit value(default value: 1000) QTECH(config)# ipv6 static route-  
limit 900
```

QTECH(config)# no ipv6 static route-limit

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table.

Platform Description

This command is not supported on 2-layer devices.

9.12. ipv6 unicast-routing

Use this command to enable the IPv6 route function of the OS. Use the **no** or **default** form of this command to disable this function.

ipv6 unicast-routing no ipv6 unicast-routing

default ipv6 unicast-routing

Parameter Description

N/A

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

Examples

Command	Description
---------	-------------

ipv6 route	Configure the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table.

Related Commands

The example disables the IPv6 route function of OS.

```
QTECH# no ipv6 unicast-routing
```

Platform Description

This command is not supported on 2-layer devices.

9.13. maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** or **default** form of this command is used to restore the default setting.

maximum-paths *number* no maximum-paths default maximum-paths

Parameter Description

Parameter	Description
<i>number</i>	Number of equivalent routes in the range from 1 to 32

Defaults

The default is 32 for routers. For switches, it depends on switch models.

Command Mode

Global configuration mode

Usage Guide

The number of equivalent routes is configured to control the number of equivalent routes. After the number of equivalent routes is configured by running the **maximum-paths** command, the number of load-sharing channels in load-sharing mode will not exceed the number of configured static routes. You can run the **show running config** command to query the number of configured static routes.

This command takes effect both to IPv4 and IPv6 addresses. After this command is configured, the maximum number of equivalent routes to an IPv4 or IPv6 destination is equal to the configured value

Examples

The following example sets the number of equivalent routes to 10 and then restores the default setting.

```
maximum-paths 10  
no maximum-paths 10
```

9.14. show ip route

Parameter

Use the commands to display the configuration of the IP routing table.

show ip route [[**vrf** *vrf_name*] [*network* [*mask* [**longer-prefix**]] | **count** | *protocol* [*process-id*] | **weight**]]

show ip route [**vrf** *vrf-name*] [[**normal** | **ecmp** | **fast-reroute**] [*network* [*mask*]]

Parameter	Description
vrf <i>vrf_name</i>	(Optional) Displays the route information of the VRF.
<i>network</i>	(Optional) Displays the route information to the network.
<i>mask</i>	(Optional) Displays the route information to the network of this mask.
longer-prefix	(optional) Displays the routes that match the specified prefix.
count	(Optional) Displays the number of existent routes. (for the ECMP/WCMP route, displays one route)
<i>protocol</i>	(Optional) Displays the route information of specific protocol.
<i>process-id</i>	(Optional) Routing protocol process ID.
weight	(Optional) Displays the route information of non default weight.
normal	Displays normal routes and not equivalent routes or fast reroutes.
ecmp	Displays only equivalent routes.
fast-reroute	(Optional) Displays the master/standby route of fast reroute.

Command Mode

Privileged EXEC mode/ Global configuration mode/Interface configuration mode/ Routing protocol configuration mode/ Route map configuration mode

Usage Guide

This command can display route information flexibly.

This command shows all routes. To show different attributes of routes, specify normal | ecmp | fast-reroute.

The following example displays the configuration of the IP routing table.

Examples

```
QTECH# show ip route
```

```
Codes: C - Connected, L - Local, S - Static
```

```
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1,  
E2 - OSPF external type 2
```

```
SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate  
default
```

```
Gateway of last resort is no set
```

```
S      20.0.0.0/8 is directly connected, VLAN 1 S      22.0.0.0/8 [1/0] via 20.0.0.1
```

```
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
```

```
R      40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
```

```
B      50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
```

```
C      192.1.1.0/24 is directly connected, VLAN 1 C 192.1.1.254/32 is local host.
```

```
QTECH# show ip route 30.0.0.0
```

```
Routing entry for 30.0.0.0/8 Distance 110, metric 20
```

```
Routing Descriptor Blocks:
```

```
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

```
QTECH# show ip route count
```

```
route info
```

```
t  n  o  acti  rout  5  
h  u  f  ve   e:  
e  m
```

```
QTECH# show ip route weight
-----[distance/metric/weight]-----
S      23.0.0.0/8 [1/0/2] via 192.1.1.20 S      172.0.0.0/16 [1/0/4] via 192.0.0.1
```

```
QTECH#show ip route normal
```

```
Codes: C - Connected, L - Local, S - Static
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
QTECH#show ip route normal
```

```
Codes: C - Connected, L - Local, S - Static
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
```

```
QTECH#show ip route ecmp
```

```
Codes: C - Connected, L - Local, S - Static
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1,
E2 - OSPF external type 2
SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate
default
Gateway of last resort is 192.168.1.2 to network 0.0.0.0 S*0.0.0.0/0      [1/0]      via
192.168.1.2
[1/0] via 192.168.2.2
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
[110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

```
QTECH#show ip route fast-reroute
```

```
Codes: C - Connected, L - Local, S - Static
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1,
E2 - OSPF external type 2
SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate
default
```

Status codes: m - main entry, b - backup entry, a - active entry

```
Gateway of last resort is 192.168.1.2 to network 0.0.0.0 S*0.0.0.0/0 [ma] via 192.168.1.2
[b] via 192.168.2.2
O IA 192.168.10.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1
[ba] via 35.1.30.2, 00:38:26, VLAN 3
```

```
QTECH# show ip route fast-reroute 30.0.0.0 Routing entry for 30.0.0.0/8
Distance 110, metric 20 Routing Descriptor Blocks:
[m] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2 [ba]192.1.1.1,
00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Field	Description	
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route	

E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Administrative distance/metric

9.15. show ip route static bfd

Use this command to display the IP route correlated BFD information

show ip route [[vrf *vrf_name*] static bfd

Parameter Description

Parameter	Description
<i>vrf vrf-name</i>	(Optional) Displays route information of the specified VRF. The default is global VRF.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the IP route correlated BFD information

```
QTECH(config)#show ip route static bfd
S      10.0.0.0/8 via 100.100.100.25, GigabitEthernet 0/3, BFD state is Up
S      20.0.0.0/8 via 200.100.100.25, GigabitEthernet 0/4, BFD state is Admin
```

The following example displays the IP route correlated BFD information,

Examples

Field	Description
S	Static route
BFD state	State of the static route correlated BFD.

Related Commands

N/A

Platform Description

This command is not supported on 2-layer devices.

9.16. show ip route summary

Use this command to display the statistical information about one routing table.

```
show ip route [vrf vrf_name] summary
```

Use this command to display the statistical information about all routing tables.

```
show ip route summary all
```

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage guideline

N/A

The following example displays the statistics of the global routing table.

```
QTECH# show ip route summary
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

Memory: 2000 bytes
Entries: 22,based on route prefixes
NORMAL ECMP FRR TOTAL
Connected 3 0 0 3
Static 2 1 1 4
RIP 1 2 1 4
OSPF 2 1 1 4
ISIS 1 2 0 3
BGP 2 1 1 4
TOTAL 11 7 4 22
```

The following example displays the statistics of all routing tables.

```
QTECH# show ip route summary all
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

IP routing table count:2 Total
Memory: 4000 bytes
Entries: 44,based on route prefixes
NORMAL ECMP FRR TOTAL
Connected 6 0 0 6
Static 4 2 2 8
RIP 2 4 2 8
OSPF 4 2 2 8
ISIS 2 4 0 6
BGP 4 2 2 8
TOTAL 22 14 8 44
```

```

Global
Memory: 2000 bytes
Entries: 22,based on route prefixes
NORMAL ECMP FRR TOTAL
Connected 3 0 0 3
Static 2 1 1 4
RIP 1 2 1 4
OSPF 2 1 1 4
ISIS 1 2 0 3
BGP 2 1 1 4
TOTAL 11 7 4 22

```

Examples

```

VRF1
Memory: 2000 bytes
Entries: 22,based on route prefixes Entries: 29,based on route nexthops
NORMAL
ECMP FRR TOTAL
Connected 3 0 0 3
Static 2 1 1 4
RIP 1 2 1 4
OSPF 2 1 1 4
ISIS 1 2 0 3
BGP 2 1 1 4
TOTAL 11 7 4 22

```

Field	Description
NORMAL	Type of the table entries. Value: NORMAL: common routes (not ECMP or FRR); ECMP: equivalent route; FRR: fast reroute; TOTAL: total
Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)

Connected	Protocol type. Value: Connected: direct connection; Static: static; RIP: RIP; OSPF: OSPF; ISIS: ISIS; BGP: BGP; TOTAL: total
-----------	---

9.17. show ip route track-table

Use this command to display the IP route correlated Track information.

show ip route [[vrf *vrf_name*] track-table

Parameter Description

Parameter	Description
vrf <i>vrf_name</i>	(Optional) Displays the route information of the specified VRF name. The default is global VRF,

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the IP route correlated Track information.

The following example displays the IP route correlated Track information.

```
QTECH(config)#show ip route track-table
ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/0 track 2 state is [up]
ip route 20.0.0.0 255.0.0.0 GigabitEthernet 0/0 2 track 3 state is [down]
```

Examples

:

Field	Description
track	Track target index
state	Track target state

Command	Description
N/A	N/A

Platform Description

This command is not supported on 2-layer devices.

9.18. show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

show ipv6 route [[**vrf** *vrf_name*] [*ipv6-prefix / prefix-length* [**longer-prefixes**] | *protocol* [*process-id*] | **weight**]]

Parameter Description

Parameter	Description
<i>vrf vrf-name</i>	(Optional) Specifies a VRF.
<i>ipv6-prefix/prefix-length</i>	(Optional) Specifies a prefix for route's IPv6 address.
<i>longer-prefixes</i>	(Optional) Displays the route with an IPv6 address prefix mostly matched.
<i>protocol</i>	((Optional) Displays the route information of specific protocol.
<i>process-id</i>	(Optional) Specifies a route process ID.
<i>weight</i>	(Optional) Displays the non-default-weight routes only.

Defaults

ll routes are displayed by default.

Command Mode

Privileged EXEC mode

```
QTECH(config)# show ipv6 route
```

```
IPv6 routing table - Default - 7 entries Codes: C - Connected, L - Local, S - Static
```

```
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1,  
E2 - OSPF external type 2
```

```
10::/64 via Loopback 1, directly connected 10::1/128 via Loopback 1, local host 20::/64  
[20/0] via 10::4, Loopback 1C FE80::/10 via Null 0, directly connected
```

```
FE80::/64 via Loopback 1, directly connected
```

The following example displays the IPv6 routing table.

Examples

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20::/64	Network address and mask of the destination network
[20/0]	Administrative distance/metric

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.

Platform Description

This command is not supported on 2-layer devices.

9.19. show ip route static bfd

Use this command to display the IPv6 route correlated BFD information

show ipv6 route [[vrf vrf_name] static bfd

Parameter Description

Parameter	Description
vrf vrf-name	(Optional) Displays the route information of the designated VRF name of the static route. The default is global VRF,

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the IPv6 route correlated BFD information.

The following example displays the IPv6 route correlated BFD information.

```
QTECH(config)#show ip route static bfd
S      25::/64 via 100::25, GigabitEthernet 0/3, BFD state is Up
S      26::/64 via 200::25, GigabitEthernet 0/4, BFD state is Admin
```

Examples

Field	Description
S	Static route
BFD state	State of the static route associated BFD

Related Commands

N/A

Platform Description

This command is not supported on 2-layer devices.

9.20. show ipv6 route summary

Use this command to display the statistics of the IPv6 routing table of a specified VRF.

`show ipv6 route [vrf vrf-name] summary`

Use this command to display statistics of all IPv6 routing tables.

`show ipv6 route summary all`

Parameter Description

Parameter	Description
<i>vrf-name</i>	(Optional) VRF name. If no VRF name is specified, statistics of the IPv6 routing table of the global VRF are displayed. .

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

```
QTECH#show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local 2
Connected 3
Static 0
PIP 0
OSPF 0
BGP 0
Total 5
```

The following example displays statistics of IPv6 routing table of the global VRF.

```
QTECH#show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local 2
Connected 3
Static 0
PIP 0
OSPF 0
BGP 0
Total 5
```

The following example displays statistics of all IPv6 routing tables.

Examples

Field	Description
Memory	The memory size occupied by the current routing table.
Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field

	can be; Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry. OSPF: OSPF route entry. ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global (The default VRF) VRF1: VRF name. TOTAL: All VRF routing table summaries.

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is not supported on 2-layer devices.

10. PROTOCOL-INDEPENDENT COMMANDS

10.1. accept-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its receiving direction. Use the no form of this command to restore the default value.

accept-lifetime *start-time* {**infinite** | *end-time* | **duration seconds**}

no accept-lifetime

Parameter description

Parameter	Description
<i>start-time</i>	Start time of the lifetime.
infinite	Indicates that the encryption key is valid for ever.
<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
duration seconds	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

Default

infinite

Command mode

Encryption key configuration mode

Usage guideline

Use this command to specify the lifetime of an encryption key in its receiving direction.

Examples

The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011.

```
QTECH(config)# key chain ripkeys QTECH(config-keychain)# key 1
QTECH(config-keychain-key)#accept-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec
12 2011
```

Related command

Command	Description
-	-

Platform - description**10.2. ip as-path access-list**

Use this command to configure an autonomous system (AS) path filter using a regular expression. Use

Parameter description

Parameter	Description
<i>path-list-num</i>	Specifies the AS-path access-list number. The range is from 1 to 500.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions.
<i>regular-expression</i>	Regular expression that defines the AS-path filter. The expression length range is from 1 to 255 characters.

the **no** form of this command to remove the AS path filter using a regular expression.

ip as-path access-list *path-list-num* { **permit** | **deny** } *regular-expression*

no ip as-path access-list *path-list-num* [{ **permit** | **deny** } *regular-expression*]

Default

By default, no AS path filter using a regular expression is configured.

Command mode

Global configuration mode

Usage guideline

N/A

Examples

The following example configures an AS path filter matching the path which contains AS number 123 only.

```
QTECH(config)# ip as-path access-list 105 deny ^123$
```


Related command

Command	Description
-	-

Platform - description

10.3. ip community-list

Use this command to define a standard or expanded community list and control access to it. Use the

no form of this command to remove the setting.

ip community-list { *community-list-number* | **standard** *community-list-name* } { **permit** | **deny** } **ip community-list** { *community-list-number* | **expanded** *community-list-name* } { **permit** | **deny** } [*regular-expression*]

Parameter description

Parameter	Description
standard	Indicates standard community list numbered in 1 to 99.
expanded	Indicates expanded community list numbered in 100 to 199.
permit	Permits access to the community list.
deny	Denies access to the community list.
<i>community-number</i>	Community number in the form of AA:NN(AS number/2-byte numerical) in the range of 1 to 255 characters. It may also be one of the following value:

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

This command is used to define the community list for BGP.

Examples

```
QTECH(config)# ip community-list standard 1 deny 100.20.200.20
QTECH(config)# ip community-list standard 1 permit internet
```

Related commands

Command	Description
match community	Match the community list.
set community-list delete	Remove the community value of the BGP path according to the community list.
show ip community-list	Show the community list information.

10.4. ip extcommunity-list

Use this command to create an extcommunity list and add an entry to the list. Use the **no** form of this command to remove the setting.

ip extcommunity-list {*expanded-list* | **expanded** *list-name* } { **permit** | **deny** } [*regular-expression*] **ip extcommunity-list** {*standard-list* | **standard** *list-name* } { **permit** | **deny** } [*rt value*] [**soo value**] **no ip extcommunity-list** {*expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name* } **ip extcommunity-list** {*expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name* }

no ip extcommunity-list {*expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name*}

Parameter description

Parameter	Description
expand-list	Indicates an extended extcommunity list, ranging from 100 to 199. One extcommunity list may contain multiple

	rules.
standard-list	Indicates a standard extcommunity list, ranging from 1 to 99. One extcommunity list may contain multiple rules.
expanded list-name	Indicates the name of an extended extcommunity, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
standard <i>list-name</i>	Indicates the name of a standard extcommunity list, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
permit	Defines an extcommunity rule for permitting.
deny	Defines an extcommunity rule for denying.
<i>regular-expression</i>	(optional) Defines a matching template that is used to match an extcommunity.
<i>sequence-number</i>	(Optional) Defines the sequence number of a rule, ranging from 1 to 2,147,483,647. If no sequence number is specified, the sequence number automatically increases by 10 when a rule is added by default. The initial number is 10.
rt	(Optional) Sets the RT attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended extcommunity configuration.
soo	(Optional) Sets the SOO attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended

	extcommunity configuration.
<i>value</i>	Indicates the value of an extended community (extend_community_value).

Default

It is disabled by default.

Command mode

Global configuration mode and ip extcommunity-list configuration mode.

Usage guidelines

This command is used to define the extcommunity list.

1. The following example defines an ip extcommunity-list.

```
QTECH(config)# ip extcommunity-list 1 permit rt 100: 1
QTECH(config)# ip extcommunity-list standard aaa permit rt 100: 2
QTECH(config)# ip extcommunity-list expanded ext1 permit 200: [0~9][0~9]
```

Examples

2. The following example displays how to use ip extcommunity.

```
QTECH(config)# route-map rt_in_filter QTECH(config-route-map)# match extcommunity 1
QTECH(config-route-map)# match extcommunity ext1 QTECH(config)# router bgp 100
QTECH(config-router)# address-family vpn
QTECH(config-router-af)#neighbor 3.3.3.3 send-community extended QTECH(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in
```

10.5. ip prefix-list

Use this command to create a prefix list or add an entry to the prefix list. Use the **no** form of this command to remove the prefix list or an entry.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix-length*]

no ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix-length*]

Parameter	Description
<i>prefix-list-name</i>	Name of the prefix list
<i>seq-number</i>	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry without a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
deny	Deny the route matching the prefix list.
permit	Permit the route matching the prefix list.
<i>ip-prefix</i>	Network address and mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and “equivalent to”.

Parameter description

Default configuration

None

Command mode

Global configuration mode

Usage guidelines

The `ip prefix-list` command configures the prefix list, with the `permit` or `deny` keyword to determine the action in case of matching.

You can execute this command to define an exact match, or use “`ge`” or “`le`” to define a range match for a prefix for flexible configuration. “`ge`” indicates the range of minimum-prefix-length to 32; “`le`” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “`ge`” and “`le`” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix <

minimum-prefix-length < maximum-prefix-length <=32.

The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24.

Examples

```
QTECH# configure terminal
QTECH(config)# ip prefix-list pre1 permit 201.1.1.0/24
QTECH(config)# router ospf
QTECH(config-router)# distribute-list prefix pre1 out rip QTECH(config-router)# end
```

10.6. ip prefix-list description

Use this command to add the description of a prefix list. Use the **no** form of this command to delete the description.

ip prefix-list *prefix-list-name* **description** *description-text*

no ip prefix-list *prefix-list-name* **description**

Parameter description

Parameter	Description
<i>prefix-list-name</i>	Name of the prefix list
<i>description-text</i>	Description of the prefix list

Default

configuration No description is added for a prefix list, by default.

Command mode Global configuration mode

The example below adds the description for the prefix list:

Examples

```
QTECH# configure terminal
QTECH(config)# ip prefix-list pre description Deny routes from Net-A
```

10.7. ip prefix-list sequence-number

Use this command to enable sort function for a prefix list. Use the **no** form of this command to disable the sort function.

ip prefix-list sequence-number

no ip prefix-list sequence-number

Parameter description

Disabled

Default configuration

No sequence number is added for a prefix list, by default.

Command mode

Global configuration mode

The example below adds a sequence number for the prefix list:

Examples

```
QTECH# configure terminal
QTECH(config)# ip prefix-list pre description deny routes from Net-A
```

Related commands

Command	Description
ip prefix-list	Configure the prefix list.

Platform description

N/A

10.8. ipv6 prefix-list

Use this command to create an IPv6 prefix list or add an entry in the prefix list. Use the **no** form of this command to delete an IPv6 prefix list or an entry in the prefix list.

ipv6 prefix-list prefix-list-name[seq seq-number] { deny | permit} ipv6-prefix [ge minimum-prefix-length][le maximum-prefix-length]


```
no ipv6 prefix-list prefix-list-name [seq seq-number] { deny | permit} ipv6-prefix [ge minimum-prefix-length][le maximum-prefix-length]
```

Parameter description

Parameter	Description
<i>prefix-list-name</i>	Name of the prefix list
<i>seq-number</i>	Sequence number of an entry in the prefix list. Its range is 1 to 4294967294. If the sequence number is not specified in this command, the system will allocate a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one is the product of adding 5 to the sequence number of the proceeding entry.
permit	Permit the access to the matching result.
deny	Deny the access to the matching result.
<i>ipv6-prefix</i>	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and “equivalent to”.

Default

No prefix list is created.

configuration

Command mode

Global configuration mode

Usage guideline

The `ipv6 prefix-list` command configures the prefix list, with the `permit` or `deny` keyword to determine the action in case of matching.

You can execute this command to define an exact match, or use “`ge`” or “`le`” to define a range match for a prefix for flexible configuration. “`ge`” indicates the range of minimum-prefix-length to 128; “`le`” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “`ge`” and “`le`” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, `Ipv6-prefix mask length <`

`minimum-prefix-length < maximum-prefix-length <= 128`

The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range `2222::/64`.

Examples

```
QTECH# configure terminal
QTECH(config)# ipv6 prefix-list pre1 permit 2222::/64
QTECH(config)# ipv6 router ospf
QTECH(config-router)# distribute-list prefix pre out rip QTECH(config-router)# end
```

10.9. ipv6 prefix-list description

Use this command to add the description of an IPv6 prefix list. Use the `no` form of this command to delete the description.

`ipv6 prefix-list prefix-lis-name description description-text`

`no ipv6 prefix-list prefix-lis-name description`

Parameter	Description
<i>prefix-lis-name</i>	Name of the ipv6 prefix list
<i>description-text</i>	Description of the ipv6 prefix list
Parameter	Description
<i>prefix-lis-name</i>	Name of the ipv6 prefix list

Parameter
description

description-text

Description of the ipv6 prefix list

Default configuration

No description is added for an IPv6 prefix list, by default.

Command mode

Global configuration mode

The example below adds the description for the prefix list:

Examples

```
QTECH# configure terminal
```

```
QTECH(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related commands

Command	Description
ipv6 prefix-list	Configure the IPv6 prefix list.

10.10. ipv6 prefix-list sequence-number

Use this command to enable the sorting function for an IPv6 prefix list. Use the **no** form of this command to remove the settings.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Parameter description

Default

configuration

No sequence number is added for a prefix list, by default.

Command mode

Global configuration mode

The example below adds a sequence number for the prefix list:

Examples

```
QTECH# configure terminal
```

```
QTECH(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related commands

Command	Description
ipv6 prefix-list	Configure the IPv6 prefix list.

10.11. key

Use this command to define an encryption key and enter the encryption key chain configuration mode. Use the no form of this command to delete it.

key *key-id*

no key *key-id*

Parameter description

Parameter	Description
<i>key-id</i>	Key ID, ranging from 0 to 2147483647.

Default

No encryption key is configured.

Command mode

Encryption key chain configuration mode.

Usage guideline

Use this command to define an encryption key.

Examples The following example configures encryption key chain ripkeys and key 1.

```
QTECH(config)# key chain ripkeys
QTECH(config-keychain)# key 1
```

Related command

Command	Description
-	-

Platform -description**10.12. key chain**

Use this command to define a key chain and enter the key chain configuration mode. Use the **no** form of this command to delete it.

key chain *key-chain-name*

no key chain *key-chain-name*

Parameter description

Parameter	Description
<i>key-chain-name</i>	Key chain name.

Default

No key chain is configured.

Command mode

Global configuration mode.

Usage

For a key chain to take effect, you need to configure at least one key.

guideline

Examples

The following example configures key chain ripkeys and enters the key chain configuration mode.

```
QTECH(config)# key chain ripkeys
```

Related command

Command	Description
---------	-------------

-

-

Platform description

10.13. key-string

Use this command to specify a key string. Use the no form of this command to delete it.

key-string [0|7] *text*

no key-string

Parameter description

Parameter	Description
0	Use plaintext.
7	Use encryption.
<i>text</i>	Authentication string.

Default

No key string is configured.

Command mode

Encryption key configuration mode.

Usage guideline

Use this command to specify a key string.

Examples

The following example configures key chain ripkeys, key 1 and the key string abc:

```
QTECH(config)# key chain ripkeys
QTECH(config-keychain)# key 1 QTECH(config-keychain-key)#key-string abc
```

Related command

Command	Description
---------	-------------

-	-
---	---

Platform description

10.14. match as-path

Use this command to redistribute the routes of AS_PATH attribute permitted by the access list in the route map configuration mode. Use the **no** form of this command to remove the setting.

match as-path *as-path-acl-list-num* [*as-path-acl-list-number*]

no match as-path [*as-path-acl-list-num*]

Parameter description

Parameter	Description
<i>as-path-acl-list-num</i>	ACL number, in the range of 1 to 500.

configuration

Command

mode Route map configuration mode.

Usage guidelines

The match as-path can be followed by an access list number or name.

One or more match or set commands can be executed to configure one route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

```
QTECH(config)# route-map ROUTEMAP2IBGP
QTECH(config-route-map)# match as-path 20 30
```

Related commands

Command	Description
match community	Match the community.

match metric	Match the metric.
match origin	Match the source of routes.
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric.
set metric-type	Set the metric type.

10.15. match community

Use this command to redistribute the routes matching the Community attribute permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match community { *community-list-number* | *community-list-name* } [**exact-match**] [{ *community-list-number* | *community-list-name* } [**exact-match**] ...]

no match community { *community-list-number* | *community-list-name* } [**exact-match**] [{ *community-list-number* | *community-list-name* } [**exact-match**] ...]

Parameter description

Parameter	Description
<i>community-list-number</i>	Number of the standard community list in the range 1 to 99. Number of the extended community list in the range of 100 to 199
<i>community-list-name</i>	Name of the community list in the range of less than 80 characters
exact-match	Match the community list exactly.

Default configuration

None.

Command mode

Route map configuration mode.

guidelines total of community lists and names should not be greater than 6. Each exact-match applies to only the previous list, not all the lists.

One or more match or set commands can be executed to configure one route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

```
QTECH(config)# ip community-list 1 permit 100:2 100:30 QTECH(config)# route-map  
set_lopref  
QTECH(config-route-map)# match community 1 exact-match  
QTECH(config-route-map)# set local-preference 20
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

10.16. match extcommunity

Use this command to define the match rule for the BGP extcommunity. Use the no form of this command to cancel the setting.

match extcommunity { *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }

no match extcommunity { *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }

Parameter description

Parameter	Description
	Standard extcommunity list number, ranging from

<i>standard-list-number</i>	1 to 99. An extcommunity list may contains multiple extcommunity values.
<i>standard-list-name</i>	Standard extcommunity name. An extcommunity list may contains multiple extcommunity values.
<i>expanded-list-num</i>	Expanded extcommunity list number, ranging from 100 to 199. An extcommunity list may contains multiple extcommunity values.
<i>expanded-list-name</i>	Expanded extcommunity name. An extcommunity list may contains multiple extcommunity values.

Default

The rule is not defined in the associated route map.

Command mode

Route map configuration mode.

Usage guideline

There are the following scenarios for a route map with an extcommunity:

The route map associated with **import map** uses the RT attribute to filter imported VRF routes.

The route maps associated with **neighbor route-map in** and **neighbor route-map out** are configured in the BGP VPNv4 address family mode and use the RT attribute to filter VPNv4 routes sent to or by BGP peers.

Examples 1.

```
QTECH(config)# ip extcommunity-list 1 permit rt 100: 1
QTECH(config)# ip extcommunity-list 1 permit rt 100: 2
```

Define two extcommunity:

```
QTECH(config)# route-map rt
QTECH(config-route-map)# match extcommunity 1
```

Define match rules in the route map:

```
QTECH(config)# router bgp 100
```

```
QTECH(config-router)# address-family vpnv4
```

```
QTECH(config-router-af)# neighbor 3.3.3.3 route-map rt in
```

Use the route map.

Related command

Command	Description
ip extcommunity-list	Create an extcommunity list.
show ip extcommunity-list	Show an extcommunity list.

Platform **-description**

10.17. match interface

Use match interface command to redistribute the routes whose next hop is the specified interface. Use the no form of this command to remove the setting.

```
match interface interface-type interface-number [...interface-type interface-number]
```

```
no match interface [interface-type interface-number [...interface-type interface-number]]
```

Parameter description

Parameter	Description
<i>interface-type</i>	Interface type
<i>interface-number</i>	Interface number

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

This command can be followed by multiple interfaces.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol.

```
router ospf
```

```
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match interface fastethernet 0/0
```

Related commands

Command	Description
match ip address	Match the address in the access list.
match ip next-hop	Match the next-hop IP address in the access list.
match ip route-source	Match the source IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.

set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.18. match ip address

Use **match ip address** command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the **no** form of this command to remove the setting.

match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name*

[*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}

no match ip address [*access-list-number* [*access-list-number...* | *access-list-name...*]

|*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]

Parameter description

Parameter	Description
<i>access-list-number</i>	Number of the access list
<i>access-list-name</i>	Name of the access list
<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow match ip address.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type-1 external type and the default metric being 40.

Examples

```
router ospf
redistribute rip subnets route-map redrip network
192.168.12.0 0.0.0.255 area 0

access-list 10 permit 200.168.23.0 0.0.0.255

route-map redrip permit 10 match ip
address 10
set metric 40
set metric-type type-1!
```

Related commands

Command	Description
access-list	Set the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop address in the access list.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.

match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.19. match ip next-hop

Use match ip next-hop command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the no form of this command to remove the setting.

match ip next-hop {*access-list-number* [*access-list-number...* | *access-list-name...*] [*access-list-name*

[*access-list-number...*]*access-list-name*] | prefix-list *prefix-list-name* [*prefix-list-name...*]}

no match ip next-hop [*access-list-number* [*access-list-number...* | *access-list-name...*]

[*access-list-name* [*access-list-number...*]*access-list-name*] | prefix-list *prefix-list-name* [*prefix-list-name*

Parameter description

Parameter	Description
<i>access-list-number</i>	Number of the access list
<i>access-list-name</i>	Name of the access list
prefix-list <i>prefix-list-name</i>	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow match ip next-hop.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to

the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip

network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 192.168.100.1
access-list 20 permit 172.16.10.1

route-map redrip permit 10 match ip
next-hop 10 20
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.

set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.20. match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list. Use the **no** form of this command to remove the setting.

match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*]
[*access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name*
[*prefix-list-name...*]}]

no match ip route-source [*access-list-number* [*access-list-number...* | *access-list-name...*]
[*access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name*
[*prefix-list-name...*]]]

Parameter description

Parameter	Description
<i>access-list-number</i>	Number of the access list
<i>access-list-name</i>	Name of the access list
<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers may follow match ip route-source.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the source IP address of the RIP route matches the access list 5, the OSPF allows for redistribution.

Examples

```
ruter ospf
redistribute rip subnets route-map redrip network
192.168.12.0 0.0.0.255 area 0

access-list 5 permit 192.168.100.1

route-map redrip permit 10 match ip
route-source 5
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.21. match ipv6 address

Use this command to redistribute the network routes permitted in the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 address { *access-list-name* } / **prefix-list** *prefix-list-name* }

no match ipv6 address

Parameter description

Parameter	Description
<i>access-list-name</i>	Name of the access list.
prefix-list <i>prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default

configuration None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list v6acl, with the default metric being 30.

Examples

```
ipv6 router ospf
redistribute rip subnets route-map redrip ipv6
access-list v6acl
10 permit ipv6 2620::64 any

route-map redrip permit 10 match ipv6
address v6acl set metric 30
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 next-hop	Match the next-hop address in the IPv6 access list.
match ipvr route-source	Match the route source address in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

10.22. match ipv6 next-hop

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 next-hop { *access-list-name* } | **prefix-list** *prefix-list-name*}

no match ipv6 next hop

Parameter description

Parameter	Description
<i>access-list-name</i>	Name of the IPv6 access list.
<i>prefix-list prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 40.

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
```

```
10 permit ipv6 2620::64 any

route-map redrip permit 10
match ipv6 address v6acl set metric
40
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.
match ipv6 route-source	Match the route source address in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

10.23. match ipv6 route-source

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 route-source { *access-list-name* } / **prefix-list** *prefix-list-name* }

no match ipv6 route-source

Parameter description

Parameter	Description
<i>access-list-name</i>	Name of the IPv6 access list.
prefix-list <i>prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 50.

Examples

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 5200::64 any

route-map redrip permit 10 match ipv6
```

```
address v6acl set metric 50
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.
match ipv6 next-hop	Match the next hop in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

10.24. match metric

Use **match metric** command to redistribute the routes of the specified metric. Use the **no** form of this command to remove the setting.

Parameter description

Parameter	Description
<i>metric</i>	Route metric, in the range 0 to 4294967295

match metric *metric*

no match metric

Default**configuration**

None.

Command mode

Route map configuration mode.

Usage guidelines

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10.

Examples

```
router ospf 1
redistribute rip subnets route-map redrip network
192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10 match
metric 10
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.

match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.25. match origin

Use this command to redistribute the routes whose source IP address is permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match origin {egp | igp | incomplete} no match origin [egp | igp | incomplete]

Parameter	Description
egp	Redistribute the routes from the remote EGP.
igp	Redistribute the routes from the local IGP.
incomplete	Redistribute the routes from an incomplete type.

Parameter description

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the origin of the routes to be redistributed. Only one origin can be set.

```
QTECH(config)# route-map MY_MAP 10 permit
QTECH(config-route-map)# match origin egp
QTECH(config-route-map)# set community 109
QTECH(config-route-map)# exit QTECH(config)# route-
```

```
map MAP20 20 permit
```

```
QTECH(config-route-map)# match origin incomplete
```

```
QTECH(config-route-map)# set community no-export
```

Examples

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set origin	Set the source.

Related commands

10.26. match route-type

Use this command to redistribute the network routes of the specified type. Use the **no** form of this command to delete the setting.

```
match route-type { static | connect | rip | local | internal | external [ type-1 | type-2 ] | level-1 |
```

Parameter	Description
local	Indicates the local route type.
static	Indicates the static route type.
connect	Indicates the directly connected route type.
rip	Indicates the RIP route type.
internal	Indicates the OSPF internal route type.
external	Indicates the OSPF external route type.
type-1 type-2	Indicates the OSPF type-1 or type-2 route

	type.
level-1 level-2	Indicates the ISIS level-1 or level-2 route type.
evpn-type-1 evpn-type-2 evpn-type-3 evpn-type-4 evpn-type-5	5 route types of BGP EVPN

Parameter description

level-2 | evpn-type-1 | evpn-type-2 | evpn-type-3 | evpn-type-4 | evpn-type-5 }

no match route-type [static | connect | rip | local | internal | external [type-1 | type-2] |
level-1 | level-2 | evpn-type-1 | evpn-type-2 | evpn-type-3 | evpn-type-4 | evpn-type-5]

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain.

Examples

```
router rip
redistribute ospf route-map redrip network
192.168.12.0

route-map redrip permit 10 match
```

```
route-type internal
```

```
!
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the access list.
set tag	Match the IP address.

10.27. match tag

Use this command to redistribute the network routes with the specified tag. Use the **no** form of this command to delete the setting.

match tag *tag* [...*tag*]

no match tag [*tag* [...*tag*]]

Parameter description

Parameter	Description
<i>tag</i>	Route tag

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Multiple tags may follow the match tag command.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain.

Examples

```
QTECH(config)# router rip
QTECH(config-router)# redistribute ospf 100 route-map redrip
QTECH(config-router)# network 192.168.12.0
QTECH(config-router)# exit
QTECH(config)# route-map
redrip permit 10
QTECH(config-route-map)# match tag 50 80
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the next-hop IP interface.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match ip next-hop	Match the next-hop IP address.
match route-type	Match the route type.

set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.28. memory-lack exit-policy

Use this command to configure a policy to preferentially exit a routing protocol when the memory reaches the lower limit. Use the **no** form of this command to restore the default policy, namely, exit the routing protocol which occupies the largest memory.

memory-lack exit-policy { bgp | ospf | pim-sm | rip }

no memory-lack exit-policy

Parameter description

Parameter	Description
bgp	Preferentially exit BGP when the memory is insufficient.
ospf	Preferentially exit OSPF when the memory is insufficient.
pim-sm	Preferentially exit PIM-SM when the memory is insufficient.
rip	Preferentially exit RIP when the memory is insufficient.

Default

By default, the routing protocol which occupies the largest memory exits preferentially.

Command mode

Global configuration mode

Usage guideline

When the memory reaches the lower limit, you can disable a routing protocol to release the memory to ensure the normal running of other protocols.

When the system runs out of memory, disable a routing protocol which has the minimal impact on the system to ensure the operation of main services.

Configuring the policy to preferentially exit the routing protocols which are disabled cannot help the system release memory.

This command ensures the operation of main services to some extent when the memory is insufficient. If the memory is further consumed, all routing protocols will exit and stop running.

Examples

The following example configures a policy to preferentially exit the BGP protocol when the memory reaches the lower limit.

```
QTECH(config)# memory-lack exit-policy bgp
```

Command	Description
-	-

Related command

Platform -description

10.29. route-map

Use route-map to enter the route map configuration mode and define a route map. Use the no form of this command to remove the setting.

```
route-map route-map-name [permit | deny] [sequence-number]
```

```
no route-map route-map-name [{permit | deny}sequence-number]
```

Parameter description

Parameter	Description
route-map-name	Name of the route map. The redistribute command references the route map according to its name. Multiple routing policies can be defined in a route map, and each policy corresponds to one sequence number.
permit	(Optional) If the permit keyword is defined and the rule defined by match is met, The set command controls the redistributed routes. For policy-based routing, the set command controls the packet forwarding, and exits the route map operation. If the permit keyword is defined but the rule defined by match is not met, the system performs the routing

	policy of the second route map till the set command is executed finally.
deny	(Optional) If the deny keyword is defined and the rule defined by match is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation. If the deny keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the
	set command is executed finally.
sequence-number	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

Default configuration

None.

Command mode

Global configuration mode.

Usage guidelines

At present, the software primarily uses the route map for route redistribution and policy-based routing.

Route redistribution control

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

When you create the first route map policy, if *sequence-number* is not specified, it is 10 by default; If only one route map policy exists and *sequence-number* is not specified, no new route map policy will be created, and the existing route map policy will be accessed for configuration;

If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed.

policy-based routing

Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The match command defines packet filtering rule and the set command defines the action for the packets matching the filtering rules. The match command used includes match ip address and match length; the set command includes set ip tos, set ip precedence, set ip dscp, set ip [default] nexthop, set ip next-hop verify-availability, set [default] interface.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the hop count of 4. In the OSPF route domain, the route type is the external route type-1, the default metric is 40 and the tag is 40.

```
!  
router ospf  
  redistribute rip subnets route-map redrip network  
  192.168.12.0 0.0.0.255 area 0  
!  
!  
route-map redrip permit 10 match  
  metric 4  
  set metric 40  
  set metric-type type-1 set tag 40
```

Related commands

Command	Description
redistribute	Redistribute the routes.

10.30. send-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its send direction. Use the no form of this command to restore the default value.

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime

Parameter description

Parameter	Description
<i>start-time</i>	Start time of the lifetime.
infinite	Indicates that the encryption key is valid for ever.
<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
duration <i>seconds</i>	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

Default infinite

Command mode

Encryption key configuration mode

Usage guideline

Use this command to specify the lifetime of an encryption key in its send direction.

Examples

The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011

```
QTECH(config)# key chain ripkeys
QTECH(config-keychain)# key 1
QTECH(config-keychain-key)# send-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12
2011
```

Related command

Command	Description
-	-

Platform **-description**

10.31. set aggregator as

Use this command to specify the AS_PATH attribute for the aggregator of the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing.

set aggregator as *as-number ip_addr*

no set aggregator as [*as-number ip_addr*]

Parameter description

Parameter	Description
<i>as-number</i>	AS number of the aggregator.
<i>ip_addresses</i>	IP address of the aggregator.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the AS_PATH attribute for the matched routes in the BGP routing domain. Only one group of parameters (as-number, ip-addr) is allowed to set at a time.

Examples

```
QTECH(config)# route-map set-as-path QTECH(config-  
route-map)# match as-path 1  
QTECH(config-route-map)# set aggregator as 3 2.2.2.2
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the route metric.
match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

10.32. set as-path prepend

Use this command to specify the AS_PATH attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set as-path prepend *as-number*

no set as-path prepend

Parameter description

Parameter	Description
<i>as-number</i>	Indicates number of the AS_PATH attribute to be configured. The AS number ranges from 1 to 4294967295, and 1 to 65535.65535 in dot mode.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to configure the AS_PATH attribute for the matched routes. Up to 10 ASs can be added into the as-path for one time.

Examples

```
QTECH(config)# route-map set-as-path QTECH(config-  
route-map)# match as-path 1  
QTECH(config-route-map)# set as-path prepend 100 101 102
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the route metric.
match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

10.33. set atomic-aggregate

Use this command to set the ATOMIC-AGGREGATE attribute for routes.

set atomic-aggregate

Use the **no** form of this command to delete existing configuration.

no set atomic-aggregate

Parameter Description

Parameter	Description

N/A	N/A
-----	-----

Defaults

N/A

Command Mode

Routing map configuration mode

Default Level 14

Usage Guide

This command is used only in the BGP protocol and is used to set the ATOMIC-AGGREGATE attribute for routes.

Configuration Examples

N/A

10.34. set comm-list delete

Use this command to delete the COMMUNITY_LIST attribute for the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing.

set comm-list *community-list-number* | *community-list-name* delete no set comm-list *community-list-number* | *community-list-name* delete

Parameter	Description
<i>community-list-number</i>	Number of the community list. Standard community list number : 1-99. Extended community list number : 100-199.
<i>community-list-name</i>	Name of the community list, which should be no more than 80 characters.

Parameter description

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the community attribute value for the matched routes that will be deleted.

```
QTECH(config-router)# neighbor 172.16.233.33 remote-as 120
QTECH(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPIN in
QTECH(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out
```

Examples

Related commands

Command	Description
match as-path	Match the AS_PATH attribute value.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set local-preference	Set the local priority of the route to be redistributed.
set metric-type	Set the metric type.

10.35. set community

Use this command to specify the community for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set community {community-number[community-number...]} [**additive** | **none**] **no set community**

Parameter description

Parameter	Description
<i>community-number</i>	Community number in the form of AA:NN or a large numeral. In addition, it can be well-known community attributes like internet, local-AS, no-export and no-advertise.
additive	Increase on the original COMMUNITY attribute.
none	Set the community attribute as blank.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the community attribute for the matched route.

Examples

```
QTECH(config)# route-map SET_COMMUNITY 10 permit
QTECH(config-route-map)# match as-path 1 QTECH(config-route-map)# set community 109:10 QTECH(config-route-map)# exit
QTECH(config)# route-map SET_COMMUNITY 20 permit
QTECH(config-route-map)# match as-path 2
QTECH(config-route-map)# set community no-export
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.

set as-path prepend	Set the AS_PATH attribute.
set origin	Set the source.
set metric-type	Set the metric type.

10.36. set dampening

Use this command to specify the dampening parameters for the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Parameter description

Parameter	Description
<i>half-life</i>	Half dampening life for the reachable or unreachable route in the range of 1 to 45 minutes, 15 minutes by default
<i>reuse</i>	When the route penalty is lower than this value, the route suppression is released. It is in the range 1 to 20000, 750 by default
<i>suppress</i>	When the route penalty is higher than this value, the route is suppressed. It is in the range 1 to 20000, 2000 by default
<i>max-suppress-time</i>	Maximum duration a route can be suppressed in the range 1 to 20000 minutes, 4* half-life by default.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the dampening parameter for the matched routes.

Examples

```
QTECH(config)# route-map tag
QTECH(config-route-map)# match as path 10
QTECH(config-route-map)# set dampening 30 1500 10000 120
QTECH(config-route-map)# exit
QTECH(config)# router bgp 100
QTECH(config-router)# neighbor 172.16.233.52 route-map tag in
```

Command	Description
match as-path	Match the AS_PATH value.
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of the route to be redistributed.

Related commands

10.37. set extcomm-list delete

Use this command to delete all extcommunity values in the extcommunity list that meet the match rules. Use the **no** form of this command to delete the configuration.

set extcomm-list { *extcommunity-list-number* | *extcommunity-list-name* } **delete** **no set extcomm-list** { *extcommunity-list-number* | *extcommunity-list-name* } **delete**

Parameter description

Parameter	Description
-----------	-------------

<i>extcommunity-list-number</i>	<i>extcommunity-list-number</i> Standard list: ranges from 1 to 99. Expanded list: ranges from 100 to 199.
<i>extcommunity-list-name</i>	<i>extcommunity-list-name</i> It consists of a maximum of 80 characters.

Default -

Command mode

Route map configuration mode.

Usage

This command is used to delete the **extcommunity-list**.

guideline

This command applies only to policy route configuration.

Examples

```
QTECH(config)# router bgp 65530
QTECH(config-router)# neighbor 172.16.233.33 remote-as 65531
QTECH(config-router)# address-family vpnv4 unicast QTECH(config-router-af)# neighbor 172.16.233.33 activate
QTECH(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPIN in QTECH(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out QTECH(config-router)# exit
QTECH(config)# ip extcommunity-list 10 permit rt 100:10
QTECH(config)# ip extcommunity-list 10 permit rt 100:20
QTECH(config)# ip extcommunity-list 120 deny 100:50 QTECH(config)# ip extcommunity-list 120 permit 100:* QTECH(config)# route-map ROUTEMAPIN permit 10 QTECH(config-route-map)# set extcomm-list 10 delete QTECH(config-route-map)# exit
QTECH(config)# route-map ROUTEMAPOUT permit 10
QTECH(config-route-map)# set extcomm-list 120 delete
```

Related command

Command	Description
---------	-------------

ip extcommunity-list	Configure an extcommunity-list .
match as-path	Match the AS_PATH value
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set extcomm-list delete	Set delete extcommunity-list .
set local-preference	Set local preference for a reroute.

Platform - description

10.38. set extcommunity

Use this command to specify the extended COMMUNITY attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set extcommunity {rt *extend-community-value* | soo *extend-community-value*}

no set extcommunity {rt | soo }

Parameter description

Parameter	Description
rt	Specify the extended community value in the form of RT.
soo	Specify the extended community value in the form of SOO.
<i>extend-community-value</i>	Extended community value.

Default

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the extended community attribute for the matched route.

Examples

Related commands

Command	Description
match as-path	Match the AS_PATH value
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

10.39. set fast-reroute

Use this command to specify a backup outgoing fast reroute and a backup next-hop for routes that meet the match conditions. Use the no form of this command to delete the configuration.

set fast-reroute backup-interface *interface-type interface-number* [**backup-nexthop** *ip-address*]

no set fast-reroute

Parameter description

Parameter	Description
<i>interface-type interface-number</i>	Backup outgoing interface.
<i>ip-address</i>	Backup next-hop.

Default -

Command mode

Route map configuration mode.

Usage guideline

Use this command to configure IP FRR backup outgoing interface and backup next-hop. The current software version supports only one backup route. This command supports only one set of the two parameters.

This command is used for fast reroute configuration.

Examples

```
QTECH(config)# access-list 2 permit 192.168.78.0 255.255.255.0
QTECH(config)# route-map frr permit 10
QTECH(config-route-map)# match ip-address 2
QTECH(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/1 backup-
nexthop 192.168.1.2
```

Related command

Command	Description
match ip-address	Match IP address list.

Platform description

N/A

10.40. set ip default next-hop

Use this command to specify the default next-hop IP address for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip default next-hop *ip-address* [*weight*] [...*ip-address* [*weight*]]

no set ip default next-hop [*ip-address* [*weight*] [...*ip-address* [*weight*]]]

Parameter description

Parameter	Description
-----------	-------------

<i>ip-address</i>	IP address of the next hop.
<i>weight</i>	Weight of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight inputted.

Up to 32 IP addresses may follow the set ip default next-hop command.

If a weight follows ip address, up to 4 next hop IP addresses can be configured.

Note: If a weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In this mode, the weight of those next hop IP addresses whose weight is not configured is 1 by default.

Differences between set ip next-hop and set ip default next-hop: After the set ip next-hop command is configured, the policy-based routing takes precedence over the routing table; while after the set ip default next-hop command is configured, the routing table takes precedence over the policy-based routing.

Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packet will be forwarded to the nexthop set with this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded through the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

The following example forwards the packets from two different nodes through different routes.

For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to device 6.6.6.6. For the messages received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to

device 7.7.7.7. The other messages will be discarded if the software cannot find the forwarding route.

Examples

```
QTECH(config)#access-list 1 permit 1.1.1.1 0.0.0.0
QTECH(config)#access-list 2 permit 2.2.2.2 0.0.0.0
QTECH(config)#interface async 1
QTECH(config-if)#ip policy route-map equal-access
QTECH(config)#route-map equal-access permit 10 QTECH(config- route-
map)#match ip address 1 QTECH(config-route-map)#set ip default
next-hop 6.6.6.6 QTECH(config)#route-map equal-access permit 20
QTECH(config-route-map)#match ip address 2 QTECH(config-route-
map)#set ip default next-hop 7.7.7.7 QTECH(config)#route-map equal-
access permit 30 QTECH(config- route-map)#set default interface
null 0
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

Platform descriptionN/A

10.41. set ip dscp

Use this command to specify the DSCP value for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip dscp *dscp-value*

no set ip dscp

Parameter description

Parameter	Description
<i>dscp-value</i>	DSCP value

Default configuration

N/A

Command mode

Route map configuration mode

Usage guideline

N/A

Examples

N/A

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

Related commands

10.42. set ip next-hop

Use this command to specify the next-hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop *ip-address* [*weight*] [...*ip-address* [*weight*]]

no set ip next-hop [*ip-address* [*weight*] [...*ip-address* [*weight*]]]

Parameter description

Parameter	Description
<i>ip-address</i>	Indicates the next-hop IP address.
<i>weight</i>	Indicates the weight of this next hop.

Default configuration

None

Command mode

Route map configuration mode

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32.

If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

Usage guideline

If weight follows ip address, up to 4 next hop addresses can be configured.

This command can be used to set different routes for the traffic that meets different match rule. If multiple IP addresses are configured, they can be used in turn.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. After the policy-based routing is used, the device will decide how to process the packets that need be routed according to the route map, which decides the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

The following example enables policy-based routing on serial 1/0. When the interface receives the packets from 10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets from 172.16.0.0/16, they will be sent to 172.16.100.1; all other packets will be discarded.

Examples

```
QTECH(config)#interface serial 1/0
QTECH(config-if)#ip policy route-map load-balance
QTECH(config)#access-list 10 permit 10.0.0.0 0.255.255.255
QTECH(config)#access-list 20 permit 172.16.0.0 0.0.255.255
QTECH(config)#route-map load-balance permit 10 QTECH(config-route-
map)#match ip address 10
QTECH(config-route-map)#set ip next-hop 192.168.100.1
QTECH(config)#route-map load-balance permit 20 QTECH(config-
route-map)#match ip address 20 QTECH(config-route-map)#set ip
next-hop 172.16.100.1 QTECH(config)#route-map load-balance permit
30
QTECH(config-route-map)#set interface Null 0
```

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

10.43. set ip next-hop recursive

Use this command to specify the recursive next-hop IP address for data packets that match a rule.

set ip next-hop recursive *ip-address*

Use the **no** form of this command to delete the configured next-hop IP address.

no set ip next-hop recursive

Parameter Description

Parameter	Description
<i>ip-address</i>	Recursive next-hop IP address

Defaults

N/A

Command Mode

Routing map configuration mode

Default Level

14

Usage Guide

This command is used only to configure PBR. Only one **set ip next-hop recursive *ip-address***

command can be configured in one routing submap policy.

According to the policy, only static or dynamic routes that have an egress and next-hop IP address can be recursed. A route can be recursed to 32 next-hop IP addresses. Only one static route can be recursed to the next hop IP address.

Examples

The following example enables PBR on Interface serial 1/0. The interface sends the data packets from the source IP address of 10.0.0.0/8 to the recursive next-hop IP address 192.168.100.1, sends the traffic from the source network 172.16.0.0/16 to the recursive next-hop IP address 172.16.100.1, and forwards other data traffic via common routes

```
QTECH(config)#interface serial 1/0
QTECH(config-if)#ip policy route-map load-balance QTECH(config)#access-list
10 permit 10.0.0.0 0.255.255.255 QTECH(config)#access-list 20 permit
172.16.0.0 0.0.255.255
QTECH(config)#route-map load-balance permit 10
```

```
QTECH(config-route-map)#match ip address 10
QTECH(config-route-map)#set ip next-hop recursive 192.168.100.1
QTECH(config)#route-map load-balance permit 20
QTECH(config-route-map)#match ip address 20
QTECH(config-route-map)#set ip next-hop recursive 172.16.100.1
```

10.44. set ip next-hop verify-availability

Use this command to verify the availability of the next hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop verify-availability *ip-address* [**track** *track-obj-number* | **bfd** *interface-type interface-number gateway*]

no set ip next-hop verify-availability *ip-address* [**track** *track-obj-number* | **bfd** *interface-type interface-number gateway*]

Parameter	Description
<i>ip-address</i>	Indicates the next-hop IP address.
track	Judges whether the next hop is effective by using <i>Track</i> .
<i>track-object-num</i>	Indicates the track object number.
bfd	Indicates that BFD is used for neighbor detection.
<i>interface-type</i>	Configures the interface type.
<i>interface-number</i>	Configures the interface number.
<i>gateway</i>	Configures the gateway IP address, which is the neighbor IP address of BFD. If the next hop is configured as the neighbor, BFD will be used to detect the

	accessibility of the forwarding path.
--	---------------------------------------

Parameter description

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

None

Examples

```
QTECH(config)#route-map rmap permit 10
QTECH(config-route-map)#set ip next-hop verify-availability
192.168.1.2
```

The following example verifies the availability of the next hop IP address being 192.168.1.2 and the number of the object to be tracked to 1.

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.

set ip precedence

Set the priority of the packets.

10.45. set ip precedence

Use this command to set the precedence of the IP head of the packet matching the rule in the route map configuration mode. Use the no form of this command to remove the configured precedence setting.

```
set ip precedence {<0-7> | critical | flash | flash-override | immediate | internet | network | priority |
```

```
routine }
```

```
no set ip precedence
```

Parameter Description

Parameter	Description
<i>number</i>	Indicates the priority of the IP header with a number, ranging from 0 to 7. 7: critical 6: flash 5: flash-override 4: immediate 3: internet 2: network 1: priority 0: routine
<i>critical</i> <i>flash</i> <i>flash-override</i> <i>immediate</i> <i>internet</i> <i>network</i> <i>priority</i> <i>routine</i>	Priority of an IP header.

Defaults

N/A

Command Mode

Route map configuration mode

Usage guideline

With different precedence values for the IP packet head configured, the IP packets matching the PBR routing are sent according to the different precedence values.

Multiple set ip precedence commands can be executed in the route map configuration rule, but only the last one takes effect, and the precedence will be specified for the head of the IP packet matched the PBR.

The following example sets the precedence of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

Examples

```
QTECH(config)#access-list 1 permit 192.168.217.68 0.0.0.0
QTECH(config)#route-map name
QTECH(config-route-map)#match ip address 1 QTECH(config-route-map)#set ip precedence 4
QTECH(config)#interface FastEthernet 0/0
QTECH(config-if)#ip policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip tos	Set the tos for the IP packet head.

10.46. set ip tos

Use this command to set the tos of the IP head of the packet matching the rule in the route map configuration mode. Use the **no** form of this command to remove the configured tos setting.

set ip tos {<0-15> | *max-reliability* | *max-throughput* | *min-delay* | *min-monetary-cost* | *normal*}

no set ip tos

Parameter Description

Parameter	Description
number	Indicates the TOS value of an IP header with a number, ranging from 0 to 15.
max-reliability max-throughput min-delay	Priority of an IP header.
min-monetary-cost normal	

Defaults

N/A

Command mode

Route map configuration mode

Usage guideline

With different TOS values for the IP packet head configured, the IP packets matching the PBR routing are transmitted with different service qualities.

The TOS value will be specified for the head of the IP packet matched the PBR.

The following example sets the TOS value of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

Examples

```
QTECH(config)#access-list 1 permit 192.168.217.68 0.0.0.0
QTECH(config)#route-map name QTECH(config-route-map)#match ip address 1 QTECH(config-
route-map)#set ip tos 4 QTECH(config)#interface FastEthernet 0/0 QTECH(config-if)#ip
policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip precedence	Set the precedence for the IP packet head.

10.47. set ipv6 default next-hop

Use this command to specify the default next-hop IPv6 address for the IPv6 packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ipv6 default next-hop *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*] ...]
no set ipv6 default next-hop *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*] ...]

Parameter

Parameter	Description
vrf vrf-name	The next hop address belongs to the specified VRF which must be the configured IPv6 address family multi-protocol VRF.
global	The next hop address belongs to the global.
global-ipv6-address	Indicates the next-hop IPv6 address for packet forwarding. The next-hop router must be a neighbor router.
weight	Indicates the weight in the load balancing mode, ranging from 1 to 8. A larger value means larger packet traffic to be shared by the next hop.

Default configuration

None

Command mode

Route map configuration mode

With the policy-based routing applied to the interface, for the IPv6 packets matching the corresponding rules, if the usual route (that is the non default route) with the destination of this packet is not in the routing table, this packet will be forwarded to the next hop specified by the set ipv6 default next-hop command. Otherwise it is forwarded through the usual route. Noted that the match rule should be the IPv6 corresponded. If the **vrf vrf-name** parameter is specified, packets are forwarded across different VRF instances. If the **global** parameter is specified, packets are forwarded from the VRF instance to a public network. If [**vrf vrf-name** | **global**] is not specified, IPv6 packets are sent to the next hop of the VRF instance same as that of the current hop.

Usage guideline

Packets select the egress from the policy-based routing and routing table in following priority: set ipv6 next-hop;

usual route (the non default route) set ipv6 default next-hop

For the switches, this function does not take effect if the mask length is beyond 64.

If this command and the `set ipv6 next-hop verify-availability` are both configured, the next hop set by the `set ipv6 next-hop verify-availability` command will take effect preferentially.

Examples

The following example sets the default next hop of the packet with destination address `2001:0db8:2001:1760::/64` received at the interface `fastEthernet 0/0` as `2002:0db8:2003:1::95`.

```
QTECH(config)# ipv6 access-list acl_for_pbr
QTECH(config-ipv6-acl)# permit ipv6 any 2001:0db8:2001:1760::/64
QTECH(config)# route-map rm_if_0_0
```

```
QTECH(config-route-map)# match ipv6 address acl_for_pbr
QTECH(config-route-map)# set ipv6 default next-hop 2002:0db8:2003:1::95
QTECH(config)# interface FastEthernet 0/0
QTECH(config-if)# ipv6 policy route-map rm_if_0_0
```

Related commands

Command	Description
match ipv6 address	Set the matching rule of policy-based routing.
ipv6 policy route-map	Use the policy-based routing on the interface.
set ipv6 next-hop	Set the next hop of the policy-based routing.

Platform description

N/A

10.48. set ipv6 next-hop

Use this command to specify the next-hop IPv6 address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ipv6 next-hop *global-ipv6-address* [*weight*] [...*global-ipv6-address* [*weight*]]

no set ip next-hop *global-ipv6-address* [*weight*] [...*global-ipv6-address* [*weight*]]

Parameter	Description
<i>global-ipv6-address</i>	IPv6 address of the next hop. The next hop router should be the neighbor router.
<i>weight</i>	Weight of the next hop in the load balancing mode, in the range of 1 to 8.

Parameter description

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow `set ip next-hop` and the number of addresses should be less than 32.

If `weight` follows `ip address`, up to 4 next hop addresses can be configured.

If the parameter `vrf vrf-name` is specified, packets forwarding will be across the VRF. The packets will be forwarded from VRF to public network with the parameter `global` specified. If no `[vrf vrf-name | global]` is specified, forwarding the IPv6 packets will inherit the VRF, that is the nexthop belongs to the VRF that receives this IPv6 packets.

If `weight` follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

When the packets select the egress from the policy-based routing and routing table, the priorities are as follows.

`set ipv6 next-hop;`

usual route (the non default route) `set ipv6 default next-hop`

Default route.

The following example sets the next hop of the packet with destination address

2001:0db8:2001:1760::/64 received at the interface fastEthernet 0/0 as
2002:0db8:2003:1::95

Examples

```
QTECH(config)# ipv6 access-list acl_for_pbr
QTECH(config-ipv6-acl)# permit ipv6 any 2001:0db8:2001:1760::/64
QTECH(config)# route-map rm_if_0_0
QTECH(config-route-map)# match ipv6 address acl_for_pbr QTECH(config-route-map)# set
ipv6 next-hop 2002:0db8:2003:1::95
QTECH(config)# interface FastEthernet 0/0
QTECH(config-if)# ipv6 policy route-map rm_if_0_0
```

Related commands

Command	Description
match ipv6 address	Set the matching rule of policy-based routing.
ipv6 policy route-map	Use the policy-based routing on the interface.
set ipv6 next-hop	Set the next hop of the policy-based routing.

Platform description

N/A

10.49. set ipv6 next-hop verify-availability

Use this command to determine the availability of the next-hop IP address.

set ipv6 next-hop verify-availability *global-ipv6-address* [**track** *track-obj-number* | **bfd** *interface-type interface-number gateway*]

Use the **no** form of this command to delete existing configuration.

no set ip next-hop verify-availability *global-ipv6-address* [**track** *track-obj-number* | **bfd** *interface-type interface-number gateway*]

Parameter Description

Parameter	Description
-----------	-------------

<i>global-ipv6-address</i>	Specifies the next-hop IPv6 address.
<i>track</i>	Detects whether the next hop is effective by using the tracking method.
<i>track-obj-number</i>	Specifies the tracking object number.
<i>bfd</i>	Conducts neighbor detection by using BFD.
<i>interface-type</i>	Specifies the interface type.
<i>interface-number</i>	Specifies the interface number.
<i>gateway</i>	Specifies the gateway IPv6 address, that is, IPv6 address of the BFD neighbor. If the configured next hop is the neighbor, the availability of the forwarding path will be detected using BFD.

Defaults

N/A

Command Mode

Routing map configuration mode

Default Level

14

Usage Guide

This command is used only to configure PBR.

Examples

The following example enables the PBR support for BFD and detects the forwarding path to the neighbor 2001:1::2 via BFD.

```
QTECH(config)# route-map rmap permit 10
QTECH(config-route-map)# set ipv6 next-hop verify-availability 2001:1::2 bfd
FastEthernet 0/1 2001:1::2
```


10.50. set ipv6 precedence

Use this command to set the precedence of the IPv6 head of the packet matching the rule in the route map configuration mode. Use the **no** form of this command to remove the configured precedence setting.

set ipv6 precedence {number | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ipv6 precedence

Parameter description

Parameter	Description
<i>critical</i> , <i>flash</i> , <i>flash-override</i> , <i>immediate</i> , <i>internet</i> , <i>network</i> , <i>priority</i> , <i>routine</i>	The precedence type of the IPv6 head.
number	The configurable precedence range.

Default configuration

N/A

Command

mode Route map configuration mode

Usage guideline

The following example sets the precedence of IPv6 packet head as 3: Configure route-map.

Examples

```
QTECH(config)#route-map pbr-aaa permit 10
QTECH(config-route-map)# set ipv6 precedence 3
```

Related commands

Or

```
QTECH(config-route-map)# set ipv6 precedence immediate
```


Command	Description
match ipv6 address	Configure the ACL used for matching the packet in IPv6 PBR.
route-map	Use the route map of the policy-based routing.
set default interface	Set the default next-hop egress.
set interface	Set the next hop egress.
set ipv6 default next-hop	Set the default next-hop address for forwarding packets.
set ipv6 next-hop	Set the next-hop address for forwarding packet.
show ipv6 policy	Show the policy-based routing
show route-map	Show the route map configuration.

Platform description

N/A

10.51. set level

Use this command to set the level of the area where the routes matching the rule are redistributed in the route map configuration command. Use the **no** form of this command to remove the setting. **set level {level-1 | level-2 | level-1-2 | stub-area | backbone}**

no set level

Parameter Description

Parameter	Description
level-1	Indicates that the re-distribution route is advertised to ISIS Level 1.

level-2	Indicates that the re-distribution route is advertised to ISIS Level 2.
level-1-2	Indicates that the re-distribution route is advertised to ISIS Level 1 and Level 2.
stub-area	Indicates that the re-distribution route is advertised to OSPF Stub Area.
backbone	Indicates that the re-distribution route is advertised to the OSPF backbone
	area.

Default configuration

None

Command mode

Route map configuration mode

In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area.

Examples

```
QTECH(config)# router ospf
QTECH(config-router)# redistribute rip subnets route-map redrip QTECH(config-router)#
network 192.168.12.0 0.0.0.255 area 0 QTECH(config-router)# exit
QTECH(config)# route-map redrip permit 10
QTECH(config-route-map)# set level backbone
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.

match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

10.52. set local-preference

Use this command to set the **LOCAL_PREFERENCE** value for the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set local-preference *number*

no set local-preference

Parameter description

Parameter	Description
<i>number</i>	Local priority metric ranging 1 to 4294967295

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the local preference for the matched routes. Only one local preference can be set.

Examples

```
QTECH(config)# route-map SET_PREF permit 10 QTECH(config-route-map)# match as-path 1
QTECH(config-route-map)# set local-preference 6800 QTECH(config-route-map)# exit
QTECH(config)# route-map SET_PREF permit 20
QTECH(config-route-map)# match as-path 2
QTECH(config-route-map)# set local-preference 50
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

10.53. set metric

Use **set metric** to set the metric for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric [+ *metric-value* | - *metric-value* | *metric-value*]

no set metric

Parameter	Description
+	Increase based on the metric of the original route
-	Decrease based on the metric of the original route
<i>metric-value</i>	Metric for the route to be redistributed

Parameter description

Default configuration

The default metric for route redistribution varies with the routing protocol.

Command mode

Route map configuration mode

Usage guideline

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attention should be paid to the upper and lower limits of the routing protocols when you execute the `set metric`, `+ metric` or `- metric` commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more `match` or `set` commands can be executed to configure a route map. If the `match` command is not used, all the routes will be matched. If the `set` command is not used, no operation will be performed.

The following example enables the OSPF routing protocol to redistribute the RIP routes and sets the default metric to 40.

Examples

```
QTECH(config)# router ospf
QTECH(config-router)# redistribute rip subnets route-map redrip QTECH(config-router)#
network 192.168.12.0 0.0.0.255 area 0 QTECH(config-router)# exit
QTECH(config)# route-map redrip permit 10
QTECH(config-route-map)# set metric 40
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.

match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

10.54. set metric-type

Use **set metric-type** to set the type of the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric-type *type*

no set metric-type

Parameter	Description
<i>type</i>	Type of the routes to be redistributed. At present, you can set the type of the routes that the OSPF protocol redistributes.

Parameter description

Default configuration

Command

mode Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.

Examples

```
QTECH(config)# router ospf
QTECH(config-router)# redistribute rip subnets route-map redrip QTECH(config-router)#
network 192.168.12.0 0.0.0.255 area 0 QTECH(config-router)# exit
QTECH(config)# route-map redrip permit 10
QTECH(config-route-map)# set metric-type type-1
```

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set tag	Set the tag.

Related commands

10.55. set next-hop

Use this command to specify the next-hop IP address for the routes that match the rule. Use the **no** form of this command to remove the setting. This command is only used to configure routing policies. **set next-hop ip-address**

no set next-hop

Parameter description

Parameter	Description
<i>ip-address</i>	IP address of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2.

```
QTECH(config)# route-map redrip permit 10
QTECH(config-route-map)# match ip address 1
QTECH(config-route-map)# set next-hop 192.168.1.2
```

Related commands

Command	Description
match interface	Match the interface.

match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

10.56. set origin

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set origin {egp | igp | incomplete} no set origin

Parameter description

Parameter	Description
egp	Redistribute the routes from the remote EGP.
igp	Redistribute the routes from the local IGP.
incomplete	Redistribute the routes from an unknown device.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the source of the routes to be matched. Only one route source attribute can be set.

Examples

```
QTECH(config)# route-map SET_ORIGIN 10 permit
QTECH(config-route-map)# match as-path 1
QTECH(config-route-map)# set origin igp
QTECH(config-route-map)# exit
QTECH(config)# route-map SET_ORIGIN 20 permit
QTECH(config-route-map)# match as-path 2
QTECH(config-route-map)# set origin egp
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of redistributed routes.

10.57. set originator-id

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the no form of this command to remove the setting.

set originator-id *ip-address*

no set originator-id [*ip-address*]

Parameter description

Parameter	Description
<i>ip-address</i>	IP address of the originator.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the source of the routes to be matched.

Examples

```
QTECH(config)# route-map SET_ORIGIN 10 permit QTECH(config-  
route-map)# match as-path 1 QTECH(config-route-map)# set  
originator-id 5.5.5.5 QTECH(config-route-map)# exit  
QTECH(config)# route-map SET_ORIGIN 20 permit  
QTECH(config-route-map)# match as-path 2  
QTECH(config-route-map)# set originator-id 5.5.5.6
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of redistributed routes.

10.58. set tag

Use this command to set the tag for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set tag *tag*

no set tag

Parameter description

Parameter	Description
<i>tag</i>	Tag of the route to be redistributed

Default configuration

The original routing tag remains unchanged.

Command mode

Route map configuration mode

Usage guideline

This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.

Examples

```
QTECH(config)# router ospf
QTECH(config-router)# redistribute rip subnets route-map redrip
QTECH(config-router)# network 192.168.12.0 0.0.0.255 area 0
QTECH(config-router)# exit
QTECH(config)# route-map redrip permit 10
QTECH(config-route-map)# set tag 100
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.

match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.

10.59. set weight

Use this command to set the weight for the BGP routes matching filtering rules.

Use the **no** form of this command to remove the setting.

set weight *number*

no set weight

Parameter description

Parameter	Description
<i>number</i>	Weight in the range of 0 to 65535

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

This command can only be used modify the weight of a BGP route.

By default, the weight of the route learned from a neighbor is the one configured with the neighbor weight command. The weight of the locally generated route is fixed 32768.

The following example sets the weight for the BGP route learned from the neighbor 1.1.1.1 at the inbound direction to 100.

Examples

```
QTECH(config)# router bgp 1
QTECH(config-router)# neighbor 1.1.1.1 route-map nei-rmap-in in
QTECH(config-router)# exit
QTECH(config)# route-map nei-rmap-in permit 10
QTECH(config-route-map)# set weight 100
AS path access list 30 permit
^30$
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match community	Match the route community.
match metric	Match the route metric.
match origin	Match the source.
set community	Set community of the redistributed route.
set metric	Set the metric of the redistributed route.
set metric type	Set the metric type of the redistributed route.

10.60. show ip as-path-access-list

Use this command to display the configuration of AS path access lists.

show ip as-path-access-list [*num*]

Parameter description

Parameter	Description
<i>num</i>	AS path access list number.

Default

N/A

Command mode

Privileged EXEC mode

Usage guideline

N/A

Examples

The following example displays the AS path access lists.

```
QTECH# show ip as-path-access-list
```

Field	Description
AS path access list	AS path access list number
permit	Permits advertisement based on matching conditions.
^30\$	Regular expression.

Related command

Command	Description
-	-

Platform description

10.61. show ip community-list

Use **show ip community-list** command to display the community list.

show ip community-list [*community-list-number* | *community-list-name*]

Parameter description

Parameter	Description
<i>community-list-number</i>	Number of the community list.
<i>community-list-name</i>	Name of the community list.

Default configuration

None

Command mode

Privileged EXEC mode

Usage guidelines

N/A

```
QTECH# show ip community-list Community-  
list standard local permit local-AS  
Community-list standard Red-Giant permit  
0:10  
deny 0:20
```

Examples**10.62. show ip extcommunity-list**

Use this command to display the extcommunity list.

`show ip extcommunity-list [extcommunity-list-num | extcommunity-list-name]`**Parameter description**

Parameter	Description
<i>extcommunity-list-num</i>	extcommunity-list number, ranging from 1 to 199.
<i>extcommunity-list-name</i>	extcommunity-list name.

Default -**Command mode**

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode and route map configuration mode.

Usage guideline**Examples**

```
QTECH # show ip extcommunity-list Standard  
extended community-list 1  
10 permit RT:1:200  
20 permit RT:1:100
```



```
Standard extended community-list 2
 10 permit RT:1:200
Expanded extended community-list rt_filter
 13 permit 1:100
```

Related command

Command	Description
ip extcommunity-list	Create an extcommunity-list.
match extcommunity	Match an extcommunity.
set extcommunity	Set an extcommunity.

Platform description

10.63. show ip prefix-list

Use **show ip prefix-list** to display the prefix list or the entries.

show ip prefix-list [*prefix-name*]

Parameter description

Parameter	Description
<i>prefix-name</i>	Name of the prefix list.

Default configuration

The configuration information of all the prefix lists is displayed by default.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
QTECH# show ip prefix-list seq pre: 2
entries
seq 5 permit 192.168.564.0/24
seq 10 permit 192.2.2.0/24
```

10.64. show ip protocols

Use this command to display information about the status of the currently running IPv4 routing protocol.

show ip protocols [vrf *vrf-name*] { bgp | isis | ospf | rip }

Parameter Description

Parameter	Description
<i>vrf-name</i>	Specifies the VRF instance name. If it is not specified, information about the status of routing protocols in global VRF mode is displayed.
bgp	Displays information about the status of the BGP protocol.
isis	Displays information about the status of the IS-IS protocol.
ospf	Displays information about the status of the OSPF protocol.
rip	Displays information about the status of the RIP protocol.
-	Displays information about the status of all running routing protocols.

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and routing map configuration mode

Default Level 14

Usage Guide

Information about the status of only the currently running routing protocol is displayed, and the information about a routing protocol that is not running is not displayed.

```
QTECH# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
```

Examples

The following example displays the status of routing protocols running in global VRF mode.

```
Router ID 57.57.57.57
  Memory Overflow is enabled
  Router is not in overflow state now
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected, includes subnets in redistribution
    bgp, includes subnets in redistribution
  Number of areas in this router is 2: 2 normal 0 stub 0 nssa
  Routing for Networks:
    57.57.57.57 0.0.0.0 area 0
    163.18.4.0 0.0.0.255 area 0
    163.18.57.0 0.0.0.255 area 0
    192.100.1.0 0.0.0.255 area 0
    192.101.1.0 0.0.0.255 area 1
    192.102.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Distance: (default is 110)

Routing Protocol is "bgp 10"
  IGP synchronization is disabled
  Default-information originate is disabled
  Default local-preference applied to incoming route is 100
  Redistributing: connected
  Neighbor(s):
    Address AddressFamily FilrIn FilrOut DistIn DistOut RouteMapIn RouteMapOut Weight
  Distance: external 20(default) internal 200(default) local 200(default)
```

Field description:

Field	Description
Routing Protocol is "ospf 1"	Name of a routing protocol
Redistributing External Routes from	Route redistribution status of a routing protocol
Distance:	Distance information of a routing protocol

10.65. show ipv6 prefix-list

Use this command to display the information about the IPv6 prefix list or its entries.

show ipv6 prefix-list [*prefix-name*]

Parameter description

Parameter	Description
<i>prefix-name</i>	Name of the IPv6 prefix list.

Default

configuration The configuration information of all the IPv6 prefix lists is displayed.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, route protocol configuration mode, route map configuration mode

Usage guideline

If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
QTECH# show ipv6 prefix-list ipv6 prefix-list p6: 2 entries
      seq 5 permit 13::/20
      seq 10 permit 14::/20
```

10.66. show key chain

Use this command to display the key chain configuration.

show key chain [*key-chain-name*]

Parameter description

Parameter	Description
<i>key-chain-name</i>	(Optional) Display the configuration of the specified key chain.

Default The configuration information of all key chains is displayed.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and key chain configuration mode.

Usage guideline

If no key chain is specified, the configuration information of all key chains is displayed.

Examples

```
QTECH# show key chain
route-map AAA, permit, sequence 10 Match clauses:
ip address 2 Set clauses:
metric 10
QTECH(config)#show key chain key chain kc
  key 1 -- text "QTECH"
    accept-lifetime (12:11:00 May 2 2001) - (infinite)
    send-lifetime (always valid) - (always valid) [valid now]
```

Field	Description
key chain	Key chain name.
key	Key ID.
accept-lifetime	Lifetime in the accept direction.

send-lifetime	Lifetime in the send direction.
---------------	---------------------------------

Related command

Command	Description
-	-

Platform description

10.67. show route-map

Use the command to display the configuration of the route map.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
<i>route-map-name</i>	(Optional) Display the configuration information of the specified the route map.

Default configuration

The configuration information of all the route maps is displayed.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

```
QTECH# show route-map
route-map AAA, permit, sequence 10 Match
clauses:
ip address 2 Set
clauses:
metric 10
```

Examples

Field	Description
route-map	Name of the route map.
Permit	The route map contains the permit keyword.
sequence 10	Sequence number of the route map.
Match clauses	Set the matching rule. Whether to perform the set operation depends on the permit or deny keyword in the route map.
Set clauses	Set the operation when the rule is matched.