Routing Configuration Commands

Table of Contents

Chapter 1 VRF Configuration Commands 1
1.1 VRF Configuration Commands 1
1.1.1 ip vrf vrf-name 1
1.1.2 description 2
1.1.3 export map 3
1.1.4 import map 5
1.1.5 rd 6
1.1.6 route-target 8
1.1.7 ip vrf forwarding 10
1.1.8 ip vrf sitemap 12
1.1.9 show ip vrf 13
1.1.10 Syntax 13
Chapter 2 Static Route Configuration Commands 15
2.1 Static Route Configuration Commands 15
2.1.1 ip route default 15
2.1.2 ip route A.B.C.D 17
2.1.3 ip route vrf 18
2.1.4 ip route bfd 20
2.1.5 ip route load-balance 21
2.1.6 ip route-weight 22
2.1.7 ip route max-number 24
2.1.8 ip route max-paths static 25
2.1.9 show ip route 26
2.1.10 show ip fib 27
2.1.11 debug ip routing 28
Chapter 3 RIP Configuration Commands 30
3.1 RIP Configuration Commands 30
3.1.1 auto-summary 31
3.1.2 default-information originate 32
3.1.3 default-metric 33
3.1.4 ip rip authentication 34
3.1.5 ip rip md5-key 35
3.1.6 ip rip dynamic-key 36
3.1.7 ip rip password 38
3.1.8 ip rip passive 39
3.1.9 ip rip deaf 40
3.1.10 ip rip receive version 41
3.1.11 ip rip send version 42
3.1.12 ip rip v1demand 43
3.1.13 ip rip v2demand 44
3.1.14 ip rip split-horizon 45

3.1.15 ip rip process-id enable 46
3.1.16 neighbor 47
3.1.17 offset 48
3.1.18 router rip process-id 49
3.1.19 timers expire 50
3.1.20 timers holddown 51
3.1.21 timers update 52
3.1.22 timers trigger 53
3.1.23 timers peer 54
3.1.24 validate-update-source 55
3.1.25 check-zero-domain 56
3.1.26 version 57
3.1.27 distance 58
3.1.28 filter 59
3.1.29 maxinum-nexthop 60
3.1.30 input-queue 61
3.1.31 show ip rip 62
3.1.32 show ip rip process-id interface 63
3.1.33 show ip rip process-id summary 64
3.1.34 show ip rip process-id database 65
3.1.35 show ip rip process-id protocol 66
3.1.36 show ip rip process-id peer 67
3.1.37 debug ip rip database 68
3.1.38 debug ip rip packet [send | receive] 69
3.1.39 debug ip rip message 70

Chapter 4 BEIGRP Configuration Commands 71

4.1 BEIGRP Configuration Commands 71

4.1.1 auto-summary 72
4.1.2 clear ip beigrp neighbors 72
4.1.3 debug ip beigrp 73
4.1.4 debug ip beigrp fsm 74
4.1.5 debug ip beigrp neighbors 75
4.1.6 debug ip beigrp packet 76
4.1.7 debug ip beigrp transmit 78
4.1.8 default-metric 79
4.1.9 Distance 80
4.1.10 Filter 81
4.1.11 beigrp log-neighbor-changes 82
4.1.12 beigrp router-id 83
4.1.13 ip beigrp bandwidth-percent 84
4.1.14 ip beigrp hello-interval 85
4.1.15 ip beigrp hold-time 86
4.1.16 ip beigrp passive 86
4.1.17 ip beigrp split-horizon 87
4.1.18 metric weights 88
4.1.19 Network 89

4.1.20 Offset 90
4.1.21 redistribute 92
4.1.22 router beigrp 93
4.1.23 show ip beigrp interface 94
4.1.24 show ip beigrp neighbors 94
4.1.25 show ip beigrp protocol 96
4.1.26 show ip beigrp topology 97
4.1.27 show ip beigrp traffic 99

Chapter 5 OSPF Configuration Commands 100

5.1 OSPF Configuration Commands 100

5.1.1 area authentication 102
5.1.2 area default-cost 103
5.1.3 area filter 105
5.1.4 area nssa 106
5.1.5 area nssa-range 108
5.1.6 area nssa-translate-interval 110
5.1.7 area range 111
5.1.8 area stub 112
5.1.9 area virtual-link 114
5.1.10 auto-cost 116
5.1.11 bfd all-interfaces 118
5.1.12 debug ip ospf adj 119
5.1.13 debug ip ospf events 120
5.1.14 debug ip ospf flood 121
5.1.15 debug ip ospf lsa-generation 123
5.1.16 debug ip ospf packet 124
5.1.17 debug ip ospf restart 125
5.1.18 debug ip ospf retransmission 127
5.1.19 debug ip ospf spf 128
5.1.20 debug ip ospf tree 129
5.1.21 default-information originate 130
5.1.22 default-metric 131
5.1.23 distance 132
5.1.24 distance ospf 134
5.1.25 filter 135
5.1.26 graceful-restart 136
5.1.27 ip ospf authentication 137
5.1.28 ip ospf bfd 139
5.1.29 ip ospf cost 140
5.1.30 ip ospf dead-interval 140
5.1.31 ip ospf demand-circuit 141
5.1.32 ip ospf hello-interval 142
5.1.33 ip ospf message-digest-key 143
5.1.34 ip ospf mib-binding 145
5.1.35 ip ospf network 146
5.1.36 ip ospf passive 147

5.1.37 ip ospf password ... 148
5.1.38 ip ospf priority ... 149
5.1.39 ip ospf retransmit-interval ... 150
5.1.40 ip ospf transmit-delay ... 151
5.1.41 ip ospf mtu-ignore ... 151
5.1.42 limit max-ext-lsa ... 152
5.1.43 limit retransmissions ... 153
5.1.44 maximum-paths ... 153
5.1.45 neighbor ... 154
5.1.46 network area ... 156
5.1.47 redistribute ... 157
5.1.48 restart ospf ... 158
5.1.49 router-id ... 159
5.1.50 router ospf ... 160
5.1.51 show ip ospf ... 161
5.1.52 show ip ospf border-routers ... 163
5.1.53 show ip ospf database ... 164
5.1.54 show ip ospf interface ... 165
5.1.55 show ip ospf neighbor ... 167
5.1.56 show ip ospf virtual-link ... 168
5.1.57 stub-router ... 169
5.1.58 summary-address ... 170
5.1.59 timers delay-timer ... 171
5.1.60 timers hold-timer ... 172
5.1.61 timers age-timer ... 173

Chapter 6 BGP Configuration Commands ... 174

6.1 BGP Configuration Commands include: ... 174

6.1.1 address-family ipv4 ... 176
6.1.2 address-family ipv6 ... 177
6.1.3 address-family vpnv4 ... 178
6.1.4 aggregate-address ... 179
6.1.5 bgp always-compare-med ... 181
6.1.6 bgp asnotation dot ... 182
6.1.7 bgp bestpath med ... 183
6.1.8 bgp client-to-client reflection ... 184
6.1.9 bgp cluster-id ... 185
6.1.10 bgp confederation identifier ... 186
6.1.11 bgp confederation peers ... 187
6.1.12 bgp dampening ... 189
6.1.13 bgp default local-preference ... 190
6.1.14 bgp default route-target filter ... 191
6.1.15 bgp deterministic-med ... 192
6.1.16 bgp fast-external-fallover ... 193
6.1.17 bgp graceful-restart ... 194
6.1.18 bgp maxas-limit ... 195
6.1.19 bgp router-id ... 196

6.1.20 bgp update-delay 197
6.1.21 bgp redistribute-internal 198
6.1.22 clear ip bgp 199
6.1.23 debug ip bgp 200
6.1.24 distance 202
6.1.25 filter 203
6.1.26 maximum-paths 204
6.1.27 neighbor activate 205
6.1.28 neighbor advertisement-interval 206
6.1.29 neighbor allowas-in 207
6.1.30 neighbor capability orf prefix-list 208
6.1.31 neighbor default-originate 210
6.1.32 neighbor description 211
6.1.33 neighbor distribute-list 212
6.1.34 neighbor ebgp-multihop 213
6.1.35 neighbor fall-over 214
6.1.36 neighbor filter-list 215
6.1.37 neighbor maximum-prefix 217
6.1.38 neighbor next-hop-self 218
6.1.39 neighbor password 219
6.1.40 neighbor peer-group 221
6.1.41 neighbor prefix-list 222
6.1.42 neighbor remote-as 223
6.1.43 neighbor remove-private-AS 225
6.1.44 neighbor route-map 226
6.1.45 neighbor route-reflector-client 227
6.1.46 neighbor route-refresh 228
6.1.47 neighbor send-community 230
6.1.48 neighbor send-label 231
6.1.49 neighbor shutdown 232
6.1.50 neighbor soft-reconfiguration 233
6.1.51 neighbor timers 234
6.1.52 neighbor ttl-security-hop 235
6.1.53 neighbor update-source 236
6.1.54 neighbor weight 238
6.1.55 network (BGP) 239
6.1.56 redistribute(BGP) 240
6.1.57 router bgp 242
6.1.58 show ip bgp 243
6.1.59 show ip bgp community 245
6.1.60 show ip bgp ipv6 unicast 245
6.1.61 show ip bgp neighbors 247
6.1.62 show ip bgp paths 248
6.1.63 show ip bgp prefix-list 248
6.1.64 show ip bgp regexp 249
6.1.65 show ip bgp summary 250
6.1.66 synchronization 251

6.1.67 table-map ... 252
6.1.68 timers ... 253

Chapter 7 Public Routing Configuration Commands ... 255
7.1 Ip aspath-list Configuration Commands ... 255
7.1.1 ip as-path access-list ... 255
7.1.2 show ip aspath-list ... 257
7.2 ip community-list Configuration Commands ... 258
7.2.1 ip community-list ... 258
7.2.2 show ip community-list ... 260
7.3 ip prefix-list commands ... 261
7.3.1 clear ip prefix-list ... 261
7.3.2 ip prefix-list ... 262
7.3.3 ip prefix-list description ... 264
7.3.4 ip prefix-list sequence-number ... 265
7.3.5 show ip prefix-list ... 266
7.4 route-map Commands ... 268
7.4.1 route-map ... 268
7.4.2 match as-path ... 271
7.4.3 match community ... 272
7.4.4 match ip address ... 274
7.4.5 match ip next-hop ... 275
7.4.6 match ip address prefix-list ... 277
7.4.7 match length ... 279
7.4.8 match metric ... 280
7.4.9 match tag ... 281
7.4.10 on-match ... 283
7.4.11 set aggregator ... 285
7.4.12 set as-path ... 286
7.4.13 set atomic-aggregate ... 288
7.4.14 set community ... 289
7.4.15 set community-additive ... 291
7.4.16 set default ... 293
7.4.17 set interface ... 294
7.4.18 set ip default ... 295
7.4.19 set ip precedence ... 296
7.4.20 set ip tos ... 297
7.4.21 set ip next-hop ... 298
7.4.22 set local-preference ... 300
7.4.23 set metric ... 301
7.4.24 set metric-type ... 303
7.4.25 set origin ... 305
7.4.26 set tag ... 306
7.4.27 set weight ... 308
7.4.28 show route-map ... 309

Chapter 8 PBR Configuration Commands ... 312
8.1 PBR Configuration Commands ... 312

8.1.1 debug ip policy 312
8.1.2 ip policy route-map 313
8.1.3 match ip address 314
8.1.4 match length 315
8.1.5 set default interface 317
8.1.6 set interface 318
8.1.7 set ip default next-hop 319
8.1.8 set ip next-hop 320
8.1.9 route-map 321
8.1.10 ip local policy 322
8.1.11 ip policy 324
8.1.12 ip route-weight 326
8.1.13 show ip local policy 327
8.1.14 show ip policy 328
Chapter 9 Switch Routing Protocol Highpriority Configuration Commands 329
9.1 Switch Routing Protocol Highpriority Configuration Commands 329
9.1.1 switch routing-protocol-highpriority 329

Chapter 1 VRF Configuration Commands

1.1 VRF Configuration Commands

VRF Configuration Commands include:

- **ip vrf vrf-name**
- **description**
- **export map**
- **import map**
- **rd**
- **route-target**
- **ip vrf forwarding**
- **ip vrf sitemap**
- **show ip vrf**

1.1.1 ip vrf vrf-name

Syntax

To configure VRF, enter the VRF configuration mode. To return to the default setting, use the no form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Parameter

vrf-name	Name of VRF

Default value

None

Command mode

Routing configuration mode

Usage guidelines

If VRF is created, use command **ip vrf vrf-name** to enter VRF configuration mode and VRF will not be created again, vice verse.

Use command **no ip vrf vrf-name** to delete all configurations of VRF. Delete VRF table and VRF configuration of relevant ports but sitemap configuration will not be deleted.

Example

The following example shows how to create VRF named PE.

R1_config#ip vrf PE

Related command

rd

1.1.2 description

Syntax

To configure VRF description, run the following command.

description *LINE*

no **description**

Parameter

LINE	Description shall be 79 characters at most

Default value

None

Command mode

VRF configuration mode

Usage guidelines

Example

The following example shows how to configure description of VRF named PE.

R1_config#ip vrf PE

R1_config_vrf_PE#description this is description for pe vrf

Related command

ip vrf *vrf-name*

1.1.3 export map

Syntax

To configure expand attribute the route carries with which VRF sends out, run the following command. To return to the default setting, use the no form of this command.

export map *WORD*

no **export map** *WORD*

Parameter

WORD	name of route-map

Default value

None

Command mode

VRF configuration mode

Usage guidelines

When using the command **export map *WORD***, if the corresponding VRF is not configured with export map, the export map name of VRF is that of route-map. If export map is configured with a different name, the export map name of VRF is the new configured name of route-map; if VRF is configured with a same name that export map, there will be a hint: “%Warning, This entry have been configed.”

When using the command **no export map *WORD***, if the to be deleted export map name is not consistent with that of VRF, there will be a hint: “%Err, This entry is not configed”; if the to be deleted export map name is consistent with that of VRF, the export map of VRF will be deleted.

When using the command **no export map**, the corresponding VRF is configured with export map and export map of VRF will be deleted; if the corresponding VRF is not configured with export map, there will be no response.

MP-BGP route with VRF configured export map which sent out by VRF output target VPN expansion attribute.

Example

The following example shows how to configure route-map name of VRF export map of PE as pe-export-map:

R1_config#ip vrf PE

R1_config_vrf_PE#export map pe-export-map

R1_config_vrf_PE#exit

R1_config#route-map pe-export-map 10 permit

R1_config_route_map #set extcommunity rt 1:1

Related command

ip vrf vrf-name

rd

1.1.4 import map

Syntax

To configure route-map filter condition of addting to VRF routing table, run the following command. To return to the default setting, use the no form of this command.

import map *WORD*

no **import map** *WORD*

Parameter

WORD	Name of route-map

Default value

None

Command mode

VRF configuration mode

Usage guidelines

When using the command **import map *WORD***, if the corresponding VRF is not configured with **import** map, the import map name of VRF is that of route-map. If import map is configured with a different name, the import map name of VRF is the new configured name of route-map; if VRF is configured with a same name that import map, there will be a hint: “%Warning, This entry have been configed.”

When using the command **no export map *WORD***, if the to be deleted import map name is not consistent with that of VRF, there will be a hint: “%Err, This entry is not configed”; if the to be deleted import map name is consistent with that of VRF, the import map of VRF will be deleted.

When using the command **no export map**, the corresponding VRF is configured with import map and import map of VRF will be deleted; if the corresponding VRF is not configured with import map, there will be no response.

MP-BGP route with VRF configured export map which sent out by VRF output target VPN expansion attribute.

Example

The following example shows how to configure route-map name of VRF import map of PE as pe-export-map:

R1_config#ip vrf PE

R1_config_vrf_PE#import map pe-import-map

R1_config_vrf_PE#exit

R1_config#route-map pe-import-map 10 permit

R1_config_route_map # match ip address 1

R1_config_route_map #exit

R1_config#ip access-list standard 1

R1_config_std#permit 1.1.1.0 255.255.255.0

R1_config_std#exit

Related command

ip vrf vrf-name

rd

1.1.5 rd

Syntax

To configure VPN route tag of VRF, run the following command.

rd *ASN:nn or IP-address:nn*

Parameter

ASN:nn or IP-address:nn	route tag of VPN

Default value

None

Command mode

VRF configuration mode

Usage guidelines

RD with 8-byte length is consist of 2-byte domain and 6-byte domain.

The type domain determines the length of two sub-domains (manager domain and distribution value sub domain) in the value domain. At present, the type domain defines 3 values: 0, 1 and 2.

For type 0, manger sub-domain has 2 bytes while the distribution value sub-domain has 4 bytes. Manger sub-domain uses 2-byte ASN and the distribution value domain offers value spaces managed by service provider. The value space is used for offering VPN service and is related to the distributed ASN.

For type 1, manger sub-domain has 4 bytes while the distribution value sub-domain has 2 bytes. Manger sub-domain uses 1 IPv4 address and the distribution value domain offers value spaces managed by service provider. The value space is used for offering VPN service and is related to the distributed IPv4.

For type 2, manger sub-domain has 4 bytes while the distribution value sub-domain has 2 bytes. Manger sub-domain uses ASN with 4 bytes and the distribution value domain offers value spaces managed by service provider. The value space is used for offering VPN service and is related to the distributed ASN.

When using the command **rd**, if its corresponding VRF is configured with the same route tag, there is a hint: “%Warning, This entry have been configed”; if its corresponding VRF is configured with a different route tag, there is a hint: “%Warning, Do 'no ip vrf' before redefining the VRF”. If you want to change the route tag of configured VRF, you must delete VRF first and re-create it; if the corresponding VRF hasn’t configure the route tag, the route tag of VRF will become the new configured route tag.

If configuring RD on PE router, it is not required all routes in one VPN use the same RD, but it must be guaranteed that each RD is globally exclusive.

Example

The following example shows how to configure VPN route tag of VRF named PE to 1:1:

R1_config#ip vrf PE

R1_config_vrf_PE#rd 1:1

Related command

ip vrf vrf-name

1.1.6 route-target

Syntax

To configure target VPN expansion attribute, run the following command. To return to the default setting, use the no form of this command.

route-target [**export|import|both**] *ASN:nn or IP-address:nn*

no **route-target** [**export|import|both**] [*ASN:nn or IP-address:nn*]

Parameter

ASN:nn or IP-address :nn	destination VPN expansion attribute

Default value

None

Command mode

VRF configuration mode

Usage guidelines

route-target ASN:nn or IP-address:nn

The command is used to add VRF input and output target VPN expansion attribute as the configured value.

route-target export ASN:nn or IP-address:nn

The command is used to add VRF output target VPN expansion attribute as the configured value.

route-target import ASN:nn or IP-address:nn

The command is used to add VRF input target VPN expansion attribute as the configured value.

route-target both ASN:nn or IP-address:nn

The command is used to add VRF input and output target VPN expansion attribute as the configured value.

no route-target

The command is used to delete all input and output target VPN expansion attribute of VRF.

no route-target ASN:nn or IP-address:nn

The command is used to delete all input and output target VPN expansion attribute of VRF.

The command is used to delete all output target VPN expansion attribute of VRF.

no route-target export ASN:nn or IP-address:nn

The command is used to delete all output target VPN expansion attribute of VRF.

no route-target import

The command is used to delete all output target VPN expansion attribute of VRF.

no route-target import ASN:nn or IP-address:nn

The command is used to delete all input target VPN expansion attribute of VRF.

The command is used to delete all output target VPN expansion attribute of VRF.

no route-target both

The command is used to delete all output target VPN expansion attribute of VRF.

no route-target both ASN:nn or IP-address:nn

The command is used to delete the designated input and output target VPN expansion attribute of VRF.

The command **route-target** is used to configure route-target expansion attribute. If the target expansion attribute is existed, there is a hint: “%Warning, This entry have been configed.”

The command **no route-target** is used to delete the command route-target expansion attribute. If the target expansion attribute is not existed, there is a hint: “%Err, This entry is not configed.”

Using BGP expansion community attribute of BGP to limit issue of VPN routing information. The expansion community attribute works as the carrier of route attribute in BGP information.

The route received by MP-BGP can only be added to VRF only if route-target import of VRF is allowed.

When MP-BGP sending route, VRF configured route-target export taken as route-target expansion attribute of VPN route will be informed to other PE.

Example

The following example shows how to input target VPN expansion attribute of VRF named PE as 1:1:

R1_config#ip vrf PE

R1_config_vrf_PE#route-target import 1:1

Related command

ip vrf vrf-name

rd

1.1.7 ip vrf forwarding

Syntax

To relate the interface to VRF, run the following command. To return to the default setting, use the no form of this command.

ip vrf forwarding *vrf-name*

no **ip vrf forwarding** [*vrf-name*]

Parameter

vrf-name	Name of VRF

Default value

The interface is non-related to VRF.

Command mode

Interface configuration mode

Usage guidelines

ip vrf forwarding *vrf-name*

If the interface is not related to VRF, the command is used to relate the interface to VRF and delete IP address on the interface;

If the interface is related to VRF, the command is used to delete the relation between the interface and the original VRF, set up the new relation between the interface and the new VRF, and delete the interface IP address;

If the interface has been related to the same VRF, there is a hint: “%Warning, Interface type num have existed in VRF vrf-name.” Here, type means the port type, num means the interface number, vrf-name means VRF name of the interface.

no ip vrf forwarding

If the interface is not related to VRF, there is a hint: “%Warning, Interface type num not in any VRF.” Here, type means the port type, num means the interface number.

If the interface is related to VRF, delete the relation between the interface and VRF and IP address of the interface.

no ip vrf forwarding vrf-name

If there is no related VRF, there is a hint “Err, Interface type num not in VRF vrf-name.” Here, type means the port type, num means the interface number, vrf-name means VRF name of the interface.

If the interface is related to other VRF, delete the relation between the interface and VRF and IP address of the interface.

Example

The following example shows how to configure the relation between interface VLAN 1 and VRF PE:

R1_config#ip vrf PE

R1_config_vrf_PE#rd 1:1

R1_config_vrf_PE#exit

R1_config #interface vlan 1

R1_config_v1#ip vrf forwarding PE

Related command

ip vrf vrf-name

1.1.8 ip vrf sitemap

Syntax

To configure MP-BGP forwarded routing and Soo attribute of network imbedded route, run the following command. To return to the default setting, use the no form of this command.

ip vrf sitemap *WORD*

no **ip vrf sitemap** [*WORD*]

Parameter

WORD	name of route-map

Default value

None

Command mode

Interface configuration mode

Usage guidelines

The interface which configures sitemap will influence MP-BGP forwarded route and Soo attribute of network

The command is configured with sitemap which will influence MP-BGP forwarded routing and Soo attribute of network imbedded route. There is no effect on ce route learned by MP-BGP.

Example

The following example shows how to configure sitemap of vlan 1 to intf-sitemap:

R1_config #interface vlan 1

R1_config_v1#ip vrf sitemap intf-sitemap

R1_config_v1#exit

R1_config#route-map intf-sitemap 10 permit

R1_config_route_map #set extcommunity soo 1:1

Related command

ip vrf forwarding

1.1.9 show ip vrf

1.1.10 Syntax

To designate VRF information, run the following command.

show ip vrf [**brief|detail|interface**] [*WORD*]

Parameter

WORD	name of VRF

Default value

None

Command mode

Other modes except exec

Usage guidelines

show ip vrf [vrf-name]

or

show ip vrf brief [vrf-name]

The command is used to show VRF brief information.

show ip vrf detail [vrf-name]

The command is used to show details of VRF.

show ip vrf interface [vrf-name]

The command is used to show port information of the designated VRF.

Example

The following example shows how to show VRF information.

R1 #show ip vrf

Name RD Interfaces

CE 1:1 vlan1

PE 2:1

Related command

ip vrf vrf-name

Chapter 2 Static Route Configuration Commands

2.1 Static Route Configuration Commands

Static route configuration commands include:

- ip route default
- ip route A.B.C.D
- ip route vrf
- ip route bfd
- ip route load-balance
- ip route-weight
- ip route max-number
- ip route max-paths static
- show ip route
- show ip fib
- debug ip routing

2.1.1 ip route default

Syntax

To set the default route and the corresponding management distance, run **ip route default**. To cancel this settings, run **no** ip route default.

ip route default {next-hop | interface} [distance] [tag *tag*] [global] [description]

no **ip route default** {next-hop | interface} [distance] [tag *tag*] [global]

Parameters

default	Sets the default route.
next-hop	Means the next hop-IP address that is used to reach a network.

interface	Stands for the to-be-used network interface.
distance	Means the management distance (1-255), which is optional.
tag *tag*	Sets a tag, which is used for matchup and route control.
global	Next-hop address depends on the route in the global routing table.
description	Means the description for the static routing items.

Default Value

The function to generate a route is disabled.

Command Mode

Routing configuration mode

Usage Guidelines

1. This command is used to set the static route which points towards a port or the next hop. In order to avoid route loopback, we make our devices not support the next-hop recursive research of the default route. The configured next hop must be the address of the next-hop device that directly connects the local port.
2. The default route also supports to set the equivalent route.
3. Parameters of global mode only can be used in VPN static route next hop in the global routing table.
4. If a routing device has its default route configured and if the destination address of a packet cannot match up with a specific subnet route or a host route, the packet will be forwarded through the default route.
5. If a route, which points to the loopback or null0 port, is set, it usually turns into a null route.
6. The main routing table can contains up to 2K static routes.

Example

The following example shows how to set a default route that points to next hop “192.168.1.133”:

```
R-CE_config#interface vlan 1
R-CE_config_v1#ip address 192.168.1.132 255.255.255.0
R-CE_config_v1#exit
R-CE_config#ip route default 192.168.1.133
R-CE_config#
```

Related Command

ip route *A.B.C.D*

ip route vrf

2.1.2 ip route A.B.C.D

Syntax

To set a route and its management distance, run **ip route A.B.C.C mask**. To cancel this settings, run **no ip route default**.

ip route *A.B.C.D mask* {next-hop | interface} [a.b.c.d] [distance] [tag *tag*] [global] [description]

no **ip route** *A.B.C.D mask* {next-hop | interface} [a.b.c.d] [distance] [tag *tag*] [global]

Parameters

A.B.C.D	Means the IP route of the destination address.
mask	Stands for the mask of the destination address.
next-hop	Means the next hop-IP address that is used to reach a network.
interface	Stands for the to-be-used network interface.
distance	Means the management distance (1-255), which is optional.
a.b.c.d	Forwarding routing address
tag *tag*	Sets a tag, which is used for matchup and route control.
global	Next-hop address depends on the route in the global routing table.
description	Means the description for the static routing items.

Default Value

The function to generate a route is disabled.

Command Mode

Global configuration mode

Usage Guidelines

1. This command is used to set the static route which points towards a port or the next hop. In order to avoid route loopback, we make our devices not support the next-hop recursive research of the default route. The configured next hop must be the address of the next-hop device that directly connects the local port.
2. The static route or default route also supports the equivalent route.
3. Parameters of global mode only can be used in VPN static route next hop in the global routing table.
4. If a routing device has its default route configured and if the destination address of a packet cannot match up with a specific subnet route or a host route, the packet will be forwarded through the default route.
5. If a route, which points to the loopback or null0 port, is set, it usually turns into a null route.
6. The main routing table can contains up to 2K static routes. The allowable maximum number of routes is 64K.

Example

The following example shows how to set a static route that points to next hop "192.168.1.133":

```
R-CE_config#interface vlan 1
R-CE_config_v1#ip address 192.168.1.132 255.255.255.0
R-CE_config_v1#exit
R-CE_config#ip route 10.1.1.0 255.255.255.0 192.168.1.133
R-CE_config#
```

Related Command

ip route default

ip route vrf

2.1.3 ip route vrf

Syntax

To configure static route or default value route in vpn, and set the max routing capacity of VPN table, run the following command. To return to the default setting, use the no form of this command.

ip route vrf *vpn_name* { {default **|** network mask } {next-hop **|** interface} [distance] [tag *tag*] [global] [description]} **|** **max-number** *value* } no **ip route vrf** *vpn_name* {{default | network mask } {next-hop | interface} [distance] [tag *tag*] [global] [description]} | **max-number** *value*}

Parameter

vrf	Configure the default route in the corresponding VPN
vpn_name	name of the corresponding VPN
default	configure the default route
network	destination address IP route prefix
mask	destination address prefix mask
next-hop	next-hop IP address
interface	To be used network interface
distance	(optional) management distance (1 to 255)
tag *tag*	Set a tag, used for match and control the route
global	Next-hop address belongs to the route in the global routing table
description	Description of the static route entry
max-number	Configure the max route amount of VPN route entry
value	The max route amount of the routing table

Default value

No static route and default route

Command mode

Global configuration mode

Usage guidelines

1. The command is used to configure the static route designating port or next hop. For avoiding recursive query of the next-hop in the statix route, the next-hop configured must be next-hop device address of the directly connected local port.
2. The static route or default route also supports configuration of the equivalent route.
3. Parameters of global mode only can be used in VPN static route next hop in the global routing table.

4. If the route configures a default route, once the packet destination address cannot be matched to the sub-net route or the host route, the packet will be forwarded by the default route.

5. If it is configured with the route directing to loopback or Null0, it will become the black-hole route in general.

6. The max routing number in VPN table is 10K.

Example

The following example shows how to configure a static route directing to 192.168.1.133 in vpn_1:

```
R-CE_config#interface vlan 1
R-CE_config_vl1#ip vrf forward vpn_1
R-CE_config_v1#ip address 192.168.1.132 255.255.255.0
R-CE_config_v1#exit
R-CE_config#ip route vrf vpn_1 10.1.1.0 255.255.255.0 192.168.1.133
R-CE_config#
```

Related command

ip route default
ip route *A.B.C.D*

2.1.4 ip route bfd

Syntax

To enable the bidirectional link query of the static route, run the first one of the following two commands.

ip route bfd { **static** { next-hop | A.B.C.D }**|** **query** <interval> **|** **reply** <interval> }

no ip route bfd { **static** { next-hop | A.B.C.D }**|** **query** <interval> **|** **reply** <interval> }

Parameters

Parameters	Description
static	Enables the bidirectional link query of the static route.
next-hop	Enables the bidirectional link query of the static route which is urgent for network query.
A.B.C.D	Means the address of the to-be-queried gateway.
query	Sets the query interval.

reply	Means the maximum interval between sending the query packets and receiving the response packets.
interval	Means the configured interval.

Default Value

The bidirectional link query of the static route is disabled.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

The following example shows hwo to detect the static routing gateway address 1.1.1.1:

ip route 10.0.0.0 255.0.0.0 1.1.1.1

ip route bfd static next-hop

ip route bfd static 1.1.1.1

Related Command

None

2.1.5 ip route load-balance

Syntax

To set the weight route balance, run the following command. To return to the default setting, use the no form of this command.

ip route load-balance

no ip route load-balance

Parameters

None

Default Value

The load balance of the route is disabled and the route search is conducted according to the load balance of the equivalent route.

Command Mode

Global configuration mode

Usage Guidelines

If you want the route load balance is conducted according to flows, you should run ip route load-balance in global configuration mode; moreover, you have to set the route load balance on the corresponding egress.

Example

S 1.1.1.0/24 is directly connected, vlan 1

is directly connected, vlan 2

Supposed that the above-mentioned equivalent route exists and the following equivalent route needs to follow the ratio “2:3” to carry out the load balance, you should set as follows:

```
R1_config#ip route load-balance
R1_config#interface vlan 1
R1_config_v1#ip route-weight 2
R1_config_v1#exit
R1_config# interface vlan 2
R1_config_v2#ip route-weight 3
R1_config_v2#exit
```

Related Command

ip route-weight

2.1.6 ip route-weight

Syntax

To set the route weight based on the data flows on the egress port, run the first one of the following two commands.

ip route-weight *value*

no ip route-weight

Parameters

Parameters	Description
value	Designates the route weight.

Default Value

The route weight is not set by default, and if the equivalent route exists, the egress port need be selected according to the route balance mode.

Command Mode

Interface configuration mode

Usage Guidelines

If ip route load-balance is not run, this command will not take effect during unicast flow forwarding even though the route weight is set on the interface.

Example

S 1.1.1.0/24 is directly connected, vlan 1

is directly connected, vlan 2

Supposed that the above-mentioned equivalent route exists and the following equivalent route needs to follow the ratio “2:3” to carry out the load balance, you should set as follows:

```
R1_config#ip route load-balance
R1_config#interface vlan 1
R1_config_v1#ip route-weight 2
R1_config_v1#exit
R1_config#interface vlan 2
R1_config_v2#ip route-weight 3
R1_config_v2#
```

Related Command

ip route load-balance

2.1.7 ip route max-number

Syntax

To set the maximum number of routes, run the first one of the following two commands.

ip route max-number *value*

no ip route max-number

Parameters

Parameters	Description
max-number	Sets the maximum number of routes for the global routing table.
value	Means the maximum number of routes which is permitted by the routing table.

Default Value

64K

Command Mode

Global configuration mode

Usage Guidelines

None

Example

The following example shows how to set the maximum number of routes in the global routing table to 20K.

R1_config#ip route max-number 20000

Related Command

None

2.1.8 ip route max-paths static

Syntax

To set the number of max next hop of the static equivalent route, run the following command. If there is no further settings, the default value is 8.

ip route max-paths static *value*

no ip route max-number static

Parameters

Parameters	Description
value	The number of max next hop of the static equivalent route.

Default Value

8

Command Mode

Global configuration mode

Usage Guidelines

None

Example

The following example shows how to set the number of max next hop of the static equivalent route to 5:

R1_config#ip route max-paths static 5

Related Command

None

2.1.9 show ip route

Syntax

To display the contents of the routing table according to users' requirements, run the following commands for different devices.

show ip route [*A.B.C.D* **| all | detail |** protocol **| bfd | summary | vrf** *vrf_name* **| information]**

Parameters

A.B.C.D	Displays a specific route. Displays all routes that can reach address A.B.C.D.
all	Displays all routes, including those inactivated routes.
cache	Displays the status of the route cache.
summary	Displays the summary information about all activated routes.
protocol	Means the protocol name or its keyword such as connected, static, bgp, Ospf, beigrp or rip.
bfd	Means the bidirectional listening of the next hop of the static route.
vrf	Displays the VPN route.
vrf_name	Displays corresponding instance name of the VPN route.
information	Displays the global route statistics information.

Default Value

None

Command Mode

This command can be run in all modes except the EXEC mode.

Usage Guidelines

None

Example

The following example shows how to display VPN_1 route:

show ip route vrf vpn_1

Related Command

show ip fib

2.1.10 show ip fib

Syntax

To display the route in the fast forwarding table, run the following command.

show ip fib { route | vrf *vrf-name* **| summary }**

Parameters

Parameters	Description
route	Displays the route in the fast forwarding table
vrf *vrf-name*	Display the VRF route in the fast forwarding table
summary	Displays the statistics of FIB table

Default Value

None

Command Mode

This command can be run in all modes except the EXEC mode.

Usage Guidelines

1. Summary, displays the statistics of FIB table, including the number of the total routing items, the number of the routing items, the status of synchronous traversing, the received number of added and deleted information sent by the main routing module.

2. If there is a vpn route, this command will display the fast forwarding table of all vpn at the same time.

Example

None

Related Command

show ip route

2.1.11 debug ip routing

Syntax

Stand-alone routing (including distributed main control terminal) device debugging commands:

debug ip routing { bfd | memory | message | search | timer | cache | vrf *vrf_name* }

Parameters

Parameters	Description
bfd	Means the debugging information about the BFD link of the static route.
memory	Means the debugging information about memory allocation.
message	Means the debugging information about route addition and deletion.
search	Means the debugging information about route query.
timer	Means the debugging information about the timer timeout.
cache	Means the debugging information about cache change.
vrf *vrf-name*	Means to specify vrf

Default Value

No debugging information is exported.

Command Mode

EXEC

Usage Guidelines

To disable the debugging information, you should run no debug ip routing.

Example

None

Related Command

None

Chapter 3 RIP Configuration Commands

3.1 RIP Configuration Commands

RIP Configuration Commands Include:

- auto-summary
- default-information
- default-metric
- ip rip authentication
- ip rip md5-key
- ip rip dynamic-key
- ip rip passive
- ip rip deaf
- ip rip password
- ip rip receive version
- ip rip send version
- ip rip v1demand
- ip rip v2demand
- ip rip split-horizon
- ip rip process-id enable
- neighbor
- offset
- router rip
- timers expire
- timers holddown
- timers update
- validate-update-source
- version

- distance
- filter
- maximum-nexthop
- input-queue
- show ip rip
- show ip rip process-id database
- show ip rip process-id interface
- show ip rip process-id summary
- show ip rip process-id protocol
- debug ip rip database
- debug ip rip packet
- debug ip rip message

3.1.1 auto-summary

Syntax

To activate the automatic summarization function, use the auto-summary command. To turn off this function, use the no form of this command.

auto-summary

no auto-summary

Parameter

This command has no parameter or keywords.

Default value

Enabled by default

Command mode

RIP global configuration

Usage guidelines

Routing summarization reduces the amount of routing information in the routing tables and switching information. Routing Information Protocol(RIP) do not support subnet mask, therefore, if it is forwarded to subnets, routing possibly cause ambiguity. RIP Version 1 always uses routing summarizarion. If using RIP Version 2, you can turn off routing summarization by using the **no auto-summary** command. When routing summarization is off, subnets are advertised..

Example

To specify RIP version on Serial 1/0 as RIP Version 2 and turn off routing summarization function

```
router rip 1
version 2
no auto-summary
```

Related commands

version

3.1.2 default-information originate

Syntax

To generate a default route, use the default-information originate command. To disable this function , use the no form of this command..

default-information { originate | originate-safe }

no default-information

Parameter

originate: Generates a default route in the RIP local routing table without condition

originate-safe: Generates RIP local default route when there is non-RIP default routes in the master routing table

Default

Disable this function by default

Command mode

RIP Global configuration mode

Usage guidelines

After the default-information originate command is activated, the routing information(0.0.0.0/0) is accompanied when send routing updating.

Example

When send routing updating information, the default routing(0.0.0.0/0) is accompanied.

```
!
router rip 1
version 2
default-information originate
!
ip route default vlan1
!
```

3.1.3 default-metric

To set default metric values for import routing, use the default-metric command. To return the default stata, use the no form of this command..

default-metric *number*

no default-metric

Parameter

parameter	description
number	Default metric value. It has a value from 1 to 16.

Default value

1

Command mode

RIP Global configuration mode .

Usage guidelines

The default-metric command is used to set default routing metric used in importing routing of other routing protocols into Rip packets. When import routing of other protocols, use the specified default routing by default-metric if no specified routing metric.

Example

The following example shows a routing switch in autonomous system 119 using both the RIP and the OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the OSPF-derived routes a RIP metric of 8.

```
router rip 1
default-metric 8
redistribute ospf 119
```

Related commands

redistribute

default-information

3.1.4 ip rip authentication

Syntax

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the **ip rip authentication** command in interface configuration mode. To restore plain text authentication, use the no form of this command.

ip rip authentication {**simple | message-digest**}

no ip rip authentication

Parameter

parameter	description
simple	Plain text authentication.
Md5	MD5 ciphertext authentication type
Dynamic	Dynamic authentication type
Commit	Send authentication request immediately (used for immediate re-authentication after authentication configuration changes).

Default value

Disabled

Command mode

Interface configuration mode

Usage guidelines

RIP Version 1 does not support authentication.

Example

The following example configures the interface to use MD5 ciphertext authentication type:

ip rip authentication md5;

Configure interface to use dynamic ciphertext authentication:

Ip rip authentication dynamic

Related commands

ip rip password

ip rip message-digest-key

3.1.5 ip rip md5-key

Syntax

To activate authentication for RIP-2 packet and designate MD5-key ciphertext on the interface, run the following command. To return to the default setting, use the no form of this command.

ip rip md5-key *key-id* **md5** [0 | 7] *password*

no ip rip md5-key

Parameter

Parameter	Description
key-id	An identifier
Password	A designated password
0	The key is plaintext (default value)
7	The key is ciphertext

Default value

Invalid MD5 authentication

Command mode

Interface configuration mode

Usage guidelines

If there is no configuration of **ip rip md5-key key-id md5 password**, there will be no authentication.

Example

The following example shows how to configure MD5 encrypt authentication packet which belongs to mykey.

ip rip md5-key 4 md5 mykey

Related command

ip rip authentication

3.1.6 ip rip dynamic-key

Syntax

To activate authentication of RIP-2 and designate MD5 or SHA1 ciphertext authentication key, run the following command. To return to the default setting, use the no form of this command.

ip rip dynamic-key *key-id* {**md5|sha1**} [0 **|** 7] *password xxxx-xx-xx-xx:xx xx:xx*

no ip rip dynamic-key *key-id* {**md5|sha1**}

Parameter

Parameter	Description
key-id	1 identifier
{md5|sha1}	Algorithm of key corresponding to key id
[0 | 7]	Designate the key type: plaintext (0) or ciphertext (7)
Password	Designate keyword (20 bytes in maximum)
xxxx-xx-xx-xx:xx	Effective time of key corresponding to key id
xx:xx	Effective time length of key corresponding to key id

Default value

Disabled dynamic authentication

Command mode

Interface configuration mode

Usage guidelines

Generally speaking, every key is effective only in the effective time period (As its effective time is based on the system time, it is suggested that the interface neighbor time must be consistant, for instance, refer to a standard time).

If the dynamic authentication is enabled and no key is activated, only non-authenticated packet can pass the authentication.

If period of validity of key is overtime, No **key** can be updated, the length of effective time of the last key can be automatically extended, until the new key takes effect.

You can add many keys one time, the system will takes effect and lose effect according to configuration of the key.

It enables many keys taking effect. You can choose one key to execute operations when forwarding packets and verify the packet according to key id after receiving the packet.

Suggestion: The effective time length of every key is 24 hours and the one key in operation is activated and the effective time of one key is three minutes before the effective time of last key.

Example

```
ip rip dynamic-key 2 sha1 xxxxxxxxxxx 2009-3-3-9:0 24:5
ip rip dynamic-key 5 md5 xxxxxxxxx 2009-3-10-9:0 24:5
ip rip dynamic-key 6 sha1 xxxxxxxxxxxxx 2009-3-11-9:0 24:5
.
.
```

Related command

ip rip authentication

3.1.7 ip rip password

Syntax

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify the plain text authentication used on the interface, use the **ip rip password** command. Use the no form of this command to prevent authentication.

ip rip password *password*

no ip rip password

Parameter

parameter	description
password	The specified password

Default value

No authenctication

Command mode

Interface configuration mode

Usage guidelines

No authentications are carried out on interface without using the **ip rip password** command to configure any password.

Example

The following example configures interface to receive and send any plain text authentication packet that belong to password 'mykey'.

ip rip password mykey

Related commands

ip rip authentication

3.1.8 ip rip passive

Syntax

To cancel the routing switch to send routing updating on interface, use the **ip rip passive** command. To reactivate the routing updating, use the no form of this command.

ip rip passive

no ip rip passive

Parameter

None

Default value

Send routing updates on the interface.

Command mode

Interface configuration mode

Usage guidelines

If you cancel routing updating on a certain interface, a specified subnetwork will keep on announcing to other interfaces, and the routing updating that from other routing switches can be continuedly accepted and dealt with on this interface.

Example

The following example sends RIP packets updating to all interfaces (except for VLAN1) that enable RIP process 1:

```
interface vlan1
ip rip 1 enable
ip address 172.15.0.1 255.255.0.0
ip rip passive
router rip 1
```

Related commands

None

3.1.9 ip rip deaf

Syntax

To disable receiving rip protocol packet on the interface, run the following command. To return to the default setting, use the no form of this command.

ip rip deaf

no ip rip deaf

Parameter

None

Default value

Disabled

Command mode

Interface configuration mode

Usage guidelines

If the **ip rip deaf** command is used on one interface, it will continue to forward routing requirements outward and inform the routing update, but without accepting any rip protocol packet.

Example

The following example shows how to forward RIP packets update to vlan 1 but not receiving rip packets:

```
interface vlan1
ip rip 1 enable
ip address 172.16.0.1 255.255.0.0
ip rip deaf
router rip 1
```

Related command

None

3.1.10 ip rip receive version

Syntax

To specify a Routing Information Protocol (RIP) version to receive on specified interface, use the **ip rip receive version** command in interface configuration mode. To follow the global version rules, use the no form of this command.

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter

parameter	description
1	(Optional) Accepts only RIP Version 1 packets on the interface.
2	(Optional) Accepts only RIP Version 2 packets on the interface.

Default value

Accepts RIP Version 1 and RIP Version 2 packets

Command mode

Interface configuration mode

Usage guidelines

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured. You can configure the interface to receive both RIP versions.

Example

The following example configures the interface to receive both RIP Version 1 and Version 2 packets:

```
ip rip receive version 1 2
```

The following example configures the interface to receive only RIP Version 1 packets:

```
ip rip receive version 1
```

Related commands

ip rip send version

version

3.1.11 ip rip send version

Syntax

To specify a Routing Information Protocol (RIP) version to send on specified interface, use the **ip rip send version** command in interface configuration mode. To follow the global version rules, use the no form of this command.

ip rip send version [**1** | **2** | **compatibility**]

no ip rip send version

Parameter

parameter	description
1	(Optional) Sends only RIP Version 1 packets out the interface.
2	(Optional) Sends only RIP Version 2 packets out the interface.
compatibility	(Optional) Broadcasts only RIP Version 2 packets out the interface.

Default value

If there is no configured global version and there is no peer or if version cannot be determined according to rip's adaptive rules, only RIP-2 packets are send.

Command mode

Interface configuration mode

Usage guidelines

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured.

Example

The following example configures the interface to send only RIP Version 1 packets out the interface:

```
ip rip send version 1
```

The following example configures the interface to send only RIP Version 2 packets out the interface:

```
ip rip send version 2
```

Related commands

ip rip receive version

version

3.1.12 ip rip v1demand

Syntax

To forward request packets with v1 format, run the following command. To return to the default setting, use the no form of this command.

ip rip v1demand

no ip rip v1demand

Parameter

None

Default value

The command follows the set global version and interface version. If neither, it will follows the auto-adaptation principle (based on the received opposite terminal).

Command mode

Interface configuration mode

Usage guidelines

The command is used to forward request packets with v1 format. The command is non-related to version in the global mode and the version on the interface. The command is only used in forwarding request. In the normal condition, the interface and the global configuration modes are applied (such as update packet).

Example

The following example shows how to configure request packets with v1 format and RIP updated packets with v2 format:

```
ip rip v1demand
ip rip send version 2
```

Related command

Ip rip v2demand
Ip rip send
Version

3.1.13 ip rip v2demand

Syntax

To forward request packets with v2 format, run the **ip rip v2demand** command. To return to the default setting, use the **no ip rip v2demand** or **default ip rip v2demand** command.

ip rip v2demand

no ip rip v2demand

Parameter

None

Default value

The command follows the set global version and interface version. If neither, it will follow the auto-adaptation principle (based on the received opposite terminal).

Command mode

Interface configuration mode

Usage guidelines

The command is used to forward request packets with v2 format. The command is non-related to version in the global mode and the version on the interface. The command is only used in forwarding request. In the normal condition, the interface and the global configuration modes are applied (such as update packet).

Example

The following example shows how to configure request packets with v2 format and RIP updated packets with v1 format:

ip rip v2demand
ip rip send version 1

Related command

Ip rip v1demand

Ip rip send

version

3.1.14 ip rip split-horizon

Syntax

To enable the split horizon mechanism, use the **ip rip split-horizon** command in interface configuration mode. To disable the split horizon mechanism, use the no form of this command.

ip rip split-horizon {simple | poisoned}

no ip rip split-horizon {simple | poisoned}

Parameter

Parameter	Description
simple	Simple split horizon.
poisoned	Split horizon with poisoned reversal.

Default value

Default behavior varies with media type.

Command mode

Interface configuration mode

Usage guidelines

For all interfaces except those for which either Frame Relay or Switched Multimegabit Data Service (SMDS) encapsulation is enabled, the default condition for this command is **ip split-horizon**; in other words, the split horizon feature is active. If the interface configuration includes encapsulation frame-relay, then the default is for split horizon to be disabled.

Note: For networks that include links over X.25 packet switched networks (PSNs), the neighbor routing switch configuration command can be used to defeat the split horizon feature. You can as an alternative explicitly specify the **no ip rip split-horizon {simple | poisoned}** command in your configuration. However, if you do so you must similarly disable split horizon for all routing switches in any relevant multicast groups on that network.

If split horizon has been disabled on an interface and you want to enable it, use the **ip rip split-horizon {simple | poisoned}** command to restore the split horizon mechanism.

Note: In general, changing the state of the default for the **ip rip split-horizon {simple | poisoned}** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a PSN), you must disable split horizon for all routing switches and access servers in any relevant multicast groups on that network.

Example

The following simple example disables split horizon on vlan1.

```
interface vlan1
no ip rip split-horizon simple
```

Related commands

neighbor

3.1.15 ip rip process-id enable

Syntax

To set the interface relate to one RIP instance, run the following command. To return to the default setting, use the no form of this command.

ip rip *process-id* **enable**

no ip rip *process-id* **enable**

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535

Default value

None

Command mode

Interface configuration mode

Usage guidelines

When one interface is configured with this command, the interface will be binded to its corresponding rip instance, becoming rip interface of the instance and generates the direct network segment corresponding to the interface as the rip route; every interface can only connect to one RIP instance. By default the interface does not relate to any instance.

Note: If enable one to be created RIP instance on the interface, create RIP instance with the instance number and vrf of the interface; if enable an existed instance on the interface, but the port binded vrif and the designated vrf when creating the instance, the interface will not become the activation interface of RIP, until the interface vrf is consistant with the instance designated vrf.

Example

```
interface vlan1
  ip rip 1 enable
```

Related command

Router rip ***process-id*** [vrf ***name***]

3.1.16 neighbor

Syntax

To define a neighboring routing switch with which to exchange routing information, use the **neighbor** command in routing switch configuration mode. To remove an entry, use the no form of this command.

neighbor *ip-address*

no neighbor *ip-address*

Parameter

parameter	description
ip-address	IP address of a peer routing switch with which routing information will be exchanged.

Default value

No neighboring routing switches are defined.

Command mode

RIP Global configuration mode

Usage guidelines

This command permits the point-to-point (nonbroadcast) exchange of routing information in order to meet special requirements of the specified nonbroadcast network.

Example

In the following example, the neighbor routing switch configuration command permits the sending of routing updating to specific neighbors.

router rip 1

neighbor 131.108.20.4

Related commands

Router rip ***process-id***

3.1.17 offset

Syntax

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the **offset** command in routing switch configuration mode. To remove an offset list, use the no form of this command.

offset {*type number* **|** *****} {**in | out**} *access-list-name offset_value*

no offset {*type number* **|** *****} {**in | out**}

Parameter

parameter	description
In	Applies the access list to incoming metrics.
Out	Applies the access list to outgoing metrics.
access-list-name	Standard access list number to be applied.
Offset_value	Positive offset to be applied to metrics for networks matching the access list.
type	(Optional) Interface type to which the offset list is applied.
number	(Optional) Interface number to which the offset list is applied.

Default value

This command is disabled by default.

Command mode

RIP Global configuration mode

Usage guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Example

In the following example, the routing switch applies an offset of 10 to routes learned from VLAN1 that satisfies the access list abc:

offset vlan1 in abc 10

3.1.18 router rip process-id

Syntax

To configure RIP instance in the global mode, run the following command. To return to the default setting, use the no form of this command.

router rip *process-id* [vrf *vrf-name*]

no router rip *process-id* [vrf *vrf-name*]

Parameter

Parameter	Description
Process-id	Configures instance ID. The value ranges from 1 to 65535.
Vrf-name	Specify the VRF to which the RIP instance belongs.

Default value

By default no RIP instance is operated. When configuring instance, process id is not by default;

Command mode

Global configuration mode

Usage guidelines

Only RIP instance is enabled can the routing instance configuration mode is entered and all global configuration parameters of RIP instance can be configured. Configuration of parameters related to the interface does not limit to the enable of RIP instance.

Example

The following example shows how to enable RIP instance and enter the instance configuration mode.

router rip 1

Related command

ip rip *process-id* **enable**

3.1.19 timers expire

Syntax

To adjust RIP network timers, use the **timers expire** configuration command. To restore the default timers, use the no form of this command.

timers expire *interval*

no timers expire

Parameter

parameter	description
interval	Interval of time in seconds after which a route is declared invalid; it should be at least three times the value of update. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.

Default value

180 seconds

Command mode

RIP global configuration mode

Usage guidelines

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note: The current and default timer values can be seen by the **show ip rip** command.

Example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

router rip 1

timers expire 30

3.1.20 timers holddown

Syntax

To adjust RIP network timers, use the **timers holddown** configuration command. To restore the default timers, use the no form of this command.

timers holddown *second*

no timers holddown

Parameter

parameter	description
second	Interval in seconds during which routing information regarding better paths is suppressed. It should be at least three times the value of update. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 120 seconds.

Default value

120 seconds

Command mode

RIP global configuration mode

Usage guidelines

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note:

The current and default timer values can be seen by the show ip rip command.

Example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

router rip 1

timers holddown 30

3.1.21 timers update

Syntax

To adjust RIP network timers, use the **timers update** command. To restore the default timers, use the no form of this command.

timers update update

no timers update

Parameter

parameter	description
update	Rate in seconds at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.

Default value

30 seconds

Command mode

RIP global configuration mode

Usage guidelines

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note:

The current and default timer values can be seen by the **show ip rip protocol** command.

Example

In the following example, updates are broadcast every 5 seconds.

```
router rip 1
timers update 5
```

Note that by setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a big concern on faster-speed serial lines. Also, if you have many routes in your updates, you can cause the routing switches to spend an excessive amount of time processing updates.

3.1.22 timers trigger

Syntax

To adjust trigger update timer, run the following command. To return to the default setting, use the no form of this command.

timers trigger *second*

no timers trigger

Parameter

Parameter	Description
second	Time interval of trigger update (unit: s)

Default value

5s

Command mode

RIP Global configuration mode

Usage guidelines

The basic timer parameters of RIP can be adjusted. As RIP works on the asynchronous routing algorithm, it's important to set timer parameters of the routers and access routers in the network to the same.

Note:

The **show ip rip** command is used to show parameters of the current or default timer.

Example

router rip 1

timers trigger 4

3.1.23 timers peer

Syntax

To adjust peer overtime timer of RIP network, run the following command. To return to the default setting, use the no form of this command.

timers peer *second*

no timers peer

Parameter

Parameter	Description
second	Time interval of peer overtime

Default value

102s

Command mode

RIP Global configuration mode

Usage guidelines

The basic timer parameters of RIP can be adjusted. As RIP works on the asynchronous routing algorithm, it’s important to set timer parameters of the routers and access routers in the network to the same.

Note:

The **show ip rip protocol** command is used to show parameters of the current or default timer.

Example

```
router rip 1
timers peer 50
```

3.1.24 validate-update-source

Syntax

To have the software validate the source IP address of incoming routing updates for RIP routing protocols, use the **validate-update-source** configuration command. To disable this function, use the no form of this command.

validate-update-source

no validate-update-source

Parameter

This command has no parameters or keywords.

Default value

Enabled

Command mode

RIP global configuration mode

Usage guidelines

This command is only applicable to RIP and IGRP. The software ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface.

Disabling split horizon on the incoming interface will also cause the system to perform this validation check.

For unnumbered IP interfaces (interfaces configured as ip unnumbered), no checking is performed.

Example

router rip 1

no validate-update-source

3.1.25 check-zero-domain

Syntax

To check the legality of zero-domain in the routing entries receiving from the neighbor, run the following command. To return to the default setting, use the no form of this command.

check-zero-domain

no check-zero-domain

Parameter

No parameters or key words

Default value

Activated

Command mode

RIP Global configuration mode

Usage guidelines

The command is mainly used in version 1. Only the segments such as route-tag, subnet mask and next hop of the routing entries received in version 1 must be 0.

Example

router rip 1

no check-zero-domain

3.1.26 version

Syntax

To specify a RIP version used globally by the routing switch, use the version routing switch configuration command. Use the no form of this command to restore the default value.

version {1 | 2}

no version

Parameter

parameter	description
1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Default value

Send and receive rip packets according to the configuration on each port. If no version is configured on the port, select the version of peer according to the rip adaptive rules. If no peer is configured on the port, the default RIP-2 packets are sent.

Command mode

RIP global configuration mode

Usage guidelines

To specify RIP versions used on an interface basis, use the **ip rip receive version** and **ip rip send version** commands; or it will send RIP packets in terms of the global configuration version.

Example

The following example enables the software to send and receive RIP Version 2 packets:

version 2

Related commands

ip rip receive version

ip rip send version

3.1.27 distance

To define an administrative distance for RIP routes, use the **distance** command in routing switch configuration mode.

distance weight [*address mask* [*access-list-name*]]

no distance weight [*address mask* [*access-list-name*]]

Parameter

parameter	description
weight	Administrative distance. An integer from 1 to 255. It is recommended to use 10 to 255. (The values 0 to 9 are reserved for internal use.) Routes with a distance value of 255 are not installed in the routing table.)
address	(Optional) Source IP address (in four-part, dotted decimal notation)
mask	(Optional) IP address mask (in four-part, dotted decimal notation) If a certain digit is 0, software will omit the corresponding value in the address.
access-list-name	(Optional) Named access list to be applied to incoming routing updates.

Default value

120

Command mode

RIP global configuration mode

Usage guidelines

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. When the optional access list name or number is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the routing switch that supplies the routing information.

Example

The following example sets the administrative distance to 100 for the routing switch with the address 192.1.1.0/24.

```
router rip 1
distance 100 192.1.1.0 255.255.255.0
```

3.1.28 filter

Syntax

To filter for RIP routes, use the filter command.

filter { *type number* **|** * } { **in** **|** **out** } { **access-list** *access-list-name* **|** **gateway** *access-list-name* **|** **prefix-list** *prefix-list-name* }

no filter { *type number* **|** * } { **in** **|** **out** } [**access-list** *access-list-name* **|** **gateway** *access-list-name* **|** **prefix-list** *prefix-list-name*]

Parameter

parameter	description
access-list-name	Standard IP access list name. This list defines networks of which are received or suppressed in routing update.
prefix-list-name	Standard IP prefix list name. This list defines networks of which are received or suppressed in routing update.
in/out	Applies access list for in/out routing update.
type	(Optional) Interface type
number	(Optional) Indicates number of interface on which applies the access list for in/out routing update. If no interface is defined, the access list is applicabale to all in/out routing update.

Default value

Disabled

Command mode

RIP global configuration mode

Usage guidelines

Filter the route that are to be sent and received.If you use the access-list command to configure **access list** for dynamic routing protocol, you shoul use the standard access list.

example

The following example filter route 10.0.0.0/8 from vlan1:

```
router rip 1
filter vlan1 out access-list mylist
ip access-list standard mylist
```

deny 10.0.0.0 255.0.0.0

permit all

3.1.29 maxinum-nexthop

Syntax

To configure the max equivalent routing number in RIP routing information, run the following command. To return to the default setting, use the no form of this command.

maximum-nexthop *number*

no maximum-nexthop

Parameter

Parameter	Description
number	The max equivalent routing number. The value ranges from 1 to 16.

Default value

4

Command mode

RIP Global configuration mode

Usage guidelines

The command is used to set the max equivalent routing number. When learning the complete equivalent routing information (metric, distance) from many neighbors. If the number of neighbor is greater than the max value of the equivalent routing number, there will be no next hop adding to the routing table.

Example

The following example shows how to the equivalent routing number of RIP routing information is 5.

router rip 1

maximum-nexthop 5

Related command

None

3.1.30 input-queue

Syntax

To adjust the size of receiving queue, run the following command. To return to the default setting, use the no form of this command.

input-queue *number*

no input-queue

Parameter

Parameter	Description
number	Size of the receiving queue. The value ranges from 1 to 61440.

Default value

200

Command mode

Global configuration mode

Usage guidelines

The command is used to set size of the receiving queue which unit is packet. The size is suggested not to oversmall, otherwise, the routing cannot not be fully learned when quantities of routing are imput.

Example

The following example shows how to set the size of receiving queue of RIP routing information to 500.

```
router rip 1
input-queue 500
```

Related command

None

3.1.31 show ip rip

Syntax

To display RIP main information, use the show ip rip command.

show ip rip

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

User can see the current configuration status about RIP instances.according to the output of this command.

Example

The following example displays configuration parameter information about RIP:

```
Switch#show ip rip
Process: 2
  Update: 30, Expire: 180, Holddown: 120
  Input-queue: 50
  Validate-update-source: Enable
  zero-domain-check: Enable
  Neighbor List:
  interface List:
  interface Loopback0
```

Description of the displaying fields:

Field	Description

Process	Configure instance ID
Update	Interval of time at which updates are sent.
Holddown	Interval (in seconds) during which routing information regarding better paths is suppressed.
Expire	Interval of time after which a route is expired.
Input-queue	Message queue depth
Validate-update-source	Check the validity of the source address.
zero-domain-check	Check the validity of message domain.
Neighbor List	Configure the Neighbor list.
interface List	List of ports associated with the instance

3.1.32 show ip rip process-id interface

Syntax

To show all interfaces of RIP instances and status of these interfaces, use the following command.

show ip rip *process-id* interface

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show all interfaces of RIP instances and status of these interfaces.

Example

The following example shows how to show all interfaces of RIP instances and status of these interfaces.

```
Switch_config#show ip rip 1 interface
Interface Loopback7 ,vrf (0)
   Address:22.2.2.2, mask:255.255.255.0
   state:active
   Send version: V1(default)
   Receive version: V1 and V2(default)
   Passive: Disable
   v1demand: Disable
   v2demand: Disable
   deaf: Disable
   Authentication type: NULL
   MD5 authentication key: NULL
   Simple password: NULL
Interface GigaEthernet0/0 ,vrf (0)
   Address:2.2.2.1, mask:255.255.255.0
   state:active
   Send version: V1(default)
   Receive version: V1 and V2(default)
   Passive: Disable
   v1demand: Disable
   v2demand: Disable
   deaf: Disable
   Authentication type: simple
   MD5 authentication key: NULL
   Simple password: NULL
```

3.1.33 show ip rip process-id summary

Syntax

To show statistics of all routes of RIP instances, run the following command. To return to the default setting, use the no form of this command.

show ip rip *process-id* summary

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535.

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information, and show the designated statistics of all routes of RIP instances.

Example

The following example shows how to show statistics of all routes of RIP instances.

Switch_config#show ip rip 1 summary

```
*------------------- RIP Process 1 Summary Statistic ------------------*
RIP route table:
  Maximum route number :1024
  Total route number :8
  Connect route number :2
  Learn route number :4
  Redistributed route number :0
        Holddown route number :0
*------------------------------------------------------------------*
```

3.1.34 show ip rip process-id database

Syntax

To show all route information of RIP instances, run the following command.

show ip rip *process-id* database

Parameter

Parameter	Description
Process-id	Instance ID. The value ranges from 1 to 65535.

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information. It shows all routing information of RIP.

Example

The following example shows how to show all routing information o RIP.

Switch#show ip rip *process-id* database
1.0.0.0/8 auto-summary
1.1.1.0/24 directly connected Loopback1
100.0.0.0/8 via 192.1.1.2 (on Vlan1)
192.1.1.0/24 redistributed

Definitions of the above domains:

Domain	Description
Network-number/network-mask	RIP routing
Summary/connected/redistributed/ via gateway	The corresponding RIP route type
interface	Ports corresponding to RIP route

3.1.35 show ip rip process-id protocol

Syntax

To show RIP configuration information, run the following command.

show ip rip *process-id* **protocol**

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the current RIP configuration information.

Example

The following example shows how to show the configuration information of RIP protocol.

```
Switch_config_rip_1#show ip rip 1 pr
RIP 1 is Active
update interval 30(s), Invalid interval 180(s)
Holddown interval 120(s), Trigger interval 1(s), peer interval 102(s)
Automatic network summarization: Enable
Filter list:
Offset list:
Redistribute policy:
Interface send version and receive version:
Global version : default
  Interface Send-version Recv-version Nbr_number
  Loopback7 V2 V1 V2 0
  GigaEthernet0/0 V2 V1 V2 4
Distance: 0 (default is 120):
Maximum route count: 1024, Current route count:8
```

3.1.36 show ip rip process-id peer

Syntax

To show status information of RIP neighbor, run the following command.

show ip rip *process-id* **peer**

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the current status information of RIP neighbor to the user.

3.1.37 debug ip rip database

Syntax

To monitor RIP route event, run the following command.

debug ip rip database

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the event of current RIP route.

Example

The following example shows how to monitor the event of RIP route.

switch# debug ip rip database

RIP-DB: Adding 192.1.1.0/24 <metric 2> via 10.1.1.2 to RIP database

Definitions of the above domains:

Domain	Description
192.1.1.0/24	Route adding to the routing table
<metric 2>	Routing metric value
10.1.1.2	Gateway address of the learned route

3.1.38 debug ip rip packet [send | receive]

Syntax

To monitor packets RIP received, run the following command.

debug ip rip packet

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show the received and sent packets of the current RIP to the user.

Example

The following example shows how to monitor packets of RIP:

```
Switch# debug ip rip packet
RIP: send to 255.255.255.255 via Loopback1
vers 1, CMD_RESPONSE, length 24
192.1.1.0/0 via 0.0.0.0 metric 2
```

When running version 2, the following will be output:

```
RIP: send to 224.0.0.9 via Loopback1
vers 2, CMD_RESPONSE, length 24
192.1.1.0/24 via 0.0.0.0 metric 2
RIP: recv RIP from 10.1.1.2 on Vlan1
  vers 2, CMD_REQUEST, length 24
```

Definitions of the above domains

Domain	Description
Send/Recv	Packets forwarded(send) and received
to/from xx.xx.xx.xx	Destination address or source address of IP packets

via Loopback1/on Vlan1	Ports for sending or receiving packets
vers 2	Version numbers for sending or receiving packets
CMD_RESPONSE/ CMD_REQUEST	Packet type
length 24	Packet length
192.1.1.0/24	Destination network of the routing information
via 0.0.0.0	Next hop address
metric	Metric of the route

3.1.39 debug ip rip message

Syntax

To monitor RIP events, run the following command.

debug ip rip message

Parameter

None

Default value

None

Command mode

EXEC

Usage guidelines

The command is used to output information and show users to events of the current RIP, such as port address, status change and timer overtime.

Example

The following example shows how to monitor RIP packets:

```
Switch# debug ip rip message
  RIP: Update timer timeout(process 1)
```

Chapter 4 BEIGRP Configuration Commands

4.1 BEIGRP Configuration Commands

BEIGRP Configuration Commands Include:

- auto-summary
- clear ip beigrp neighbors
- debug ip beigrp
- debug ip beigrp fsm
- debug ip beigrp neighbours
- debug ip beigrp packet
- debug ip beigrp transmit
- default-metric
- distance
- filter
- beigrp log-neighbor-changes
- beigrp router-id
- ip beigrp bandwidth-percent
- ip beigrp hello-interval
- ip beigrp hold-time
- ip beigrp passive
- ip beigrp split-horizon
- metric weights
- network
- offset
- redistribute
- router beigrp
- show ip beigrp interface

- show ip beigrp neighbors
- show ip beigrp protocol
- show ip beigrp topology
- show ip beigrp traffic

4.1.1 auto-summary

Syntax

The auto summary is disabled by default. Since auto summary is currently not supported to enable, this command has no form only.

no auto-summary

Parameter

None

default

Disabled

Command mode

Router configuration

Usage guidelines

None

related commands

None

4.1.2 clear ip beigrp neighbors

Syntax

To delete entries from the neighbor table, use the **clear ip beigrp** command in EXEC mode.

clear ip beigrp [*as-number*] **neighbors** [*ip-address* **|** *interface*-type *interface-number*]

Parameter

parameter	description
as_number	(Optional) Neighbor's autonomous system number.
ip-address	(Optional) Address of BEIGRP's neighbor.
interface	(Optional) Interface name. After typing this parameter, all neighbors on this interface will perform adjacent reset.

default

none

Command mode

EXEC

Usage guidelines

All BEIGRP's neighbors will be reset without specifying any parameter.

The use of this command will lead adjacent reset of one or several neighbors, and then triggers routing operation. In the case when many routes are influenced, it may cause route fluctuation, and it needs some time to convergence again. So we recommend not to use this command unless the system is in the network debugging stage.

Example

The following example removes all neighbors on vlan 1 and triggers recalculation of the related routes:

```
clear ip beigrp neighbors vlan 1
```

4.1.3 debug ip beigrp

Syntax

To trace BEIGRP protocol information, you can press this command in the privileged EXEC mode.

debug ip beigrp

no debug ip beigrp

parameter

none

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command.

Example

debug ip beigrp

4.1.4 debug ip beigrp fsm

Syntax

To trace the change of state machine of BEIGRP DUAL algorithm, use the debug ip beigrp fsm command in EXEC command.

debug ip beigrp fsm

Parameter

none

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command

Related commands

debug ip beigrp packets

4.1.5 debug ip beigrp neighbors

Syntax

To display the establishment and deletion of BEIGRP neighbors, use the debug ip beigrp neighbors command in EXEC mode.

debug ip beigrp neighbors

Parameter

None

Default

None

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command.

example

TestC#debug ip beigrp neighbors

BEIGRP: Neighbor 192.168.20.141 went down on vlan 1 for peer restarted.

BEIGRP: Neighbor(192.168.20.141) not yet found.

BEIGRP: Neighbor(192.168.20.141) not yet found.

BEIGRP: New neighbor 192.168.20.141

BEIGRP: Neighbor 202.117.80.143 went down on vlan 2 for manually cleared.

BEIGRP: Neighbor 192.168.20.141 went down on vlan 1 for manually cleared.

BEIGRP: New neighbor 192.168.20.204

BEIGRP: New neighbor 202.117.80.143

BEIGRP: New neighbor 192.168.20.141

related commands

debug ip beigrp fsm

4.1.6 debug ip beigrp packet

Syntax

To display BEIGRP packets situations, use the debug ip beigrp packet command in EXEC mode.

debug ip beigrp packets [**ack** | **hello** | **query** | **reply** | **retry** | **terse** | **update** | **error**]

no debug ip beigrp packets [**ack** | **hello** | **query** | **reply** | **retry** | **terse** | **update** | **error**]

Parameter

parameter	description
ack	(Optional) Traces ACK pacekts
hello	(Optional) Traces hello packets.
query	(Optional) Traces query packets.
reply	(Optional) Traces reply packets
retry	(Optional) Traces retry packets.
terse	(Optional) Traces all packets except hello packets.
update	(Optional) Traces update packets.
error	(Optional) Traces error packets.

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command.

example

router#debug ip beigrp packet

BEIGRP: Send HELLO packet to 224.0.0.10 via vlan 2 with Ack 0/0

BEIGRP: Receive ACK packet from 192.168.20.141 via vlan 1 with Ack 0/54
BEIGRP: Receive HELLO packet from 202.117.80.143 via vlan 2 with Ack 0/0
BEIGRP: Receive UPDATE packet from 192.168.20.204 via vlan 1 with Ack 142/0
BEIGRP: Send HELLO packet to 192.168.20.204 via vlan 1 with Ack 0/142
BEIGRP: Receive HELLO packet from 192.168.20.141 via vlan 1 with Ack 0/0
BEIGRP: Receive HELLO packet from 192.168.20.204 via vlan 1 with Ack 0/0
BEIGRP: Receive QUERY packet from 192.168.20.204 via vlan 1 with Ack 143/0
BEIGRP: Send HELLO packet to 192.168.20.204 via vlan 1 with Ack 0/143
BEIGRP: Send REPLY packet to 192.168.20.204 via vlan 1 with Ack 55/143
BEIGRP: Send UPDATE packet to 224.0.0.10 via vlan 2 with Ack 57/0
BEIGRP: Receive ACK packet from 192.168.20.204 via vlan 1 with Ack 0/55
BEIGRP: resend UPDATE packet for neighbor 192.168.20.204 with retry num 1.
BEIGRP: Receive ACK packet from 202.117.80.143 via vlan 2 with Ack 0/57
BEIGRP: Send UPDATE packet to 202.117.80.143 via vlan 2 with Ack 57/77
BEIGRP: Send UPDATE packet to 224.0.0.10 via vlan 1 with Ack 56/0
BEIGRP: Receive ACK packet from 192.168.20.204 via vlan 1 with Ack 0/56
BEIGRP: Send UPDATE packet to 192.168.20.141 via vlan 1 with Ack 56/88
BEIGRP: Send UPDATE packet to 192.168.20.204 via vlan 1 with Ack 56/143
BEIGRP: Receive UPDATE packet from 202.117.80.143 via vlan 2 with Ack 79/0
BEIGRP: Send HELLO packet to 202.117.80.143 via vlan 2 with Ack 0/79
BEIGRP: Receive ACK packet from 192.168.20.204 via vlan 1 with Ack 0/56
BEIGRP: Send QUERY packet to 224.0.0.10 via vlan 1 with Ack 60/0
BEIGRP: Send UPDATE packet to 224.0.0.10 via vlan 1 with Ack 61/0

FIeld	Description
Recv / Send / Enqueueing	Receives, sends or enqueueings packet to send -queue
HELLO / UPDATE / QUERY / ACK	Packet types that are received or sent.
192.1.1.1	Neighbor IP address to send packet
vlan 2	In or out interface of packet
Ack 56/88	Acknowledgement number of packet/ sequence number of neighbor packet

related commands

debug ip beigrp fsm

4.1.7 debug ip beigrp transmit

Syntax

To display transmit event of BEIGRP packet, use the debug ip beigrp transmit command in EXEC mode.

debug ip beigrp transmit [**ack | build | link | packetize | peerdown | startup**]

no debug ip beigrp transmit [**ack | build | link | packetize | peerdown | startup**]

Parameter

parameter	description
ack	(Optional) Traces events
build	(Optional)Traces BUILD events.
link	(Optional)Traces LINK events
packetize	(Optional)Traces PACKETIZE events.
peerdown	(Optional)Traces PEERDOWN events
startup	(Optional)Traces STARTUP events.

default

none

Command mode

EXEC

Usage guidelines

It helps to find network malfunction using this command.

related commands

debug ip beigrp fsm

4.1.8 default-metric

Syntax

To reset the default vector metric for the Enhanced Interior Gateway Routing Protocol (BEIGRP), use the **default-metric** command. To restore the default state, use the no form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric

Parameter

parameter	description
bandwidth	Default bandwidth
delay	Default interface delay.
reliability	Default interface reliability
loading	Default interface load
mtu	The default value for the maximum transmission unit (MTU),

default

bandwidth: 128kpbs

delay: 2000 (10ms)

reliability: 255 (255 indicates 100%)

loading: 255 (255 indicates 100%)

mtu: 1500

Command mode

router configuration

Usage guidelines

it is generally used with redistribute command to specify default metrics of route of other routing protocols assigned into BEIGRP. This command will trigger the new algorithm of related route that are previously assigned into BEIGRP.

Forwarding static route, straight connected route and BEIGRP protocol route, you can not configure default-metric command, or you must configure this command

Example

The following example shows how the redistributed Routing Information Protocol (RIP) metrics are translated into EIGRP metrics with values as follows: bandwidth = 200, delay = 100, reliability = 100, loading = 200, and MTU = 1500:

default-metric 200 1000 100 200 1500

related commands

redistribute

4.1.9 Distance

Syntax

To allow the use of two administrative distances (internal and external) that could be a better route to a node, use the distance beigrp command in routing switch configuration mode. To reset these values to their defaults, use the no form of this command.

distance beigrp *internal-distance external-distance*

no distance beigrp

distance weight *ip-address ip-address-mask* [*ip-access-list*]

no distance weight *ip-address ip-address-mask* [*ip-access-list*]

Parameter

parameter	description
internal-distance	Administrative distance for Enhanced Internal Gateway Routing Protocol (BEIGRP) internal routes. The distance can be a value from 1 to 255.
external-distance	Administrative distance for EIGRP external routes. The distance can be a value from 1 to 255.
ip-address	BEIGRP neighbor IP address
ip-address-mask	BEIGRP neighbor IP address mask
ip-access-list	BEIGRP neighbor access list

default

internal-distance: 90

external-distance: 170

Command mode

router configuration

Usage guidelines

An administrative distance is to compare the priority of routes of different protocols. Therefore, adjustment on the administrative distance value of BEIGRP will affect the choice of routing switch to meet different demands od users

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list.

Example

```
router beigrp 2
network 192.10.0.0 255.255.0.0
distance beigrp 100 200
distance 110 192.31.7.0 255.255.255.0
distance 220 128.88.1.0 255.255.255.0
```

In the above example, the routing switch beigrp global configuration command sets up BEIGRP internal administrative and external administrative to 100 and 200. The network routing switch configuration commands specify BEIGRP routing on networks 192.31.7.0/24 and 128.88.1.0/24 to 110 and 220.

related commands

show ip protocol

4.1.10 Filter

Syntax

To allows us to filter the routes that learned or sent on the specified interface, use the filter command. Use the no form of this command to disable filter.

filter {*interface*-type *interface*-number **|** *} {**in** **|** **out**} {**access-list** *access-list-name* **|** **gateway** *access-list-name* **|** **prefix-list** *prefix-list-name*}

no filter {*interface*-type *interface*-number **|** *} {**in** **|** **out**} {**access-list** *access-list-name* **|** **gateway** *access-list-name* **|** **prefix-list** *prefix-list-name*}

Parameter

parameter	description
interface-type	Interface type and number

interface-number	
*	all intefaces
in	Applies access-list to the incoming routing update
out	Applies access-list to the ourcoming routing update
access-list	Applies standard access list to filter routes, to define which network is sent and which network is suppressed in routing update.
gateway	Filters gateway of route using standard access list.
access-list-name	Standard IP access list number or name
prefix-list	Filters route using the prefix-list
prefix-list-name:	Standard IP prefix- list-name. This list defines which networks are received and which are surpressed.

default

none

Command mode

router configuration

Usage guidelines

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list.

example

The following example permits only one network at 131.108.0.0 to be declared by BEIGRP routing process:

```
  ip access-list standard 1
   permit 131.108.0.0 255.255.0.0
  !
  router beigrp 64
   filter * out access-list 1
 network 131.108.0.0
```

4.1.11 beigrp log-neighbor-changes

Syntax

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (BEIGRP) neighbor adjacencies, use the beigrp log-neighbor-changes command in router configuration mode. To disable the logging of changes in BEIGRP neighbor adjacencies, use the no form of this command.

beigrp log-neighbor-changes

no beigrp log-neighbor-changes

Parameter

none

default

disabled

Command mode

router configuration

4.1.12 beigrp router-id

Syntax

To set the routing switch ID used by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the eigrp router-id command in router configuration mode. To remove the configured routing switch ID, use the no form of this command.

beigrp router-id *ip-address*

no beigrp router-id

Parameter

parameter	description
ip-address	Router ID in dotted decimal notation.

default

EIGRP automatically selects an IP address to use as the routing switch ID. Set the largest loopback interface as the routing switch ID if there is a loopback interface or set the largest direct-connect interface address as the the routing switch ID.

Command mode

router configuration

4.1.13 ip beigrp bandwidth-percent

Syntax

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (BEIGRP) on an interface, use the ip bandwidth-percent eigrp command. To restore the default value, use the no form of this command.

ip beigrp bandwidth-percent *percent*

no ip beigrp bandwidth-percent

parameter

parameter	description
percent	Percent of bandwidth that EIGRP may use.

default

50%

Command mode

interface configuration mode

Usage guidelines

For low speed lines, you can adjust the configuration of this command to restrict the enabled bandwidth for BEIGRP to avoid that BEIGRP affect the normal data transmission. .

Example

```
interface vlan 1
ip beigrp bandwidth-percent 100
```

The above example allows BEIGRP to use all bandwidth of the interface vlan 1.

related commands

bandwidth

4.1.14 ip beigrp hello-interval

Syntax

To configure the hello interval for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the ip hello-interval eigrp command in interface configuration mode. To restore the default value, use the no form of this command.

ip beigrp hello-interval *seconds*

no ip beigrp hello-interval

Parameter

parameter	description
second	Hello interval (in seconds).

default

5 seconds-

Command mode

interface configuration mode

Usage guidelines

example

interface vlan 1

ip beigrp hello-interval 20

The above example sets 20 seconds as the hello interval for vlan 1:

related commands

ip beigrp hold-time

4.1.15 ip beigrp hold-time

Syntax

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (BEIGRP) process, use the ip hold-time eigrp command in interface configuration mode. To restore the default value, use the no form of this command.

ip beigrp hold-time *seconds*

no ip beigrp hold-time

Parameter

parameter	description
second	Hold time is in seconds if do not receive any BEIGRP

default

15 seconds

Command mode

interface configuration mode

Usage guidelines

example

Interface vlan 1

ip beigrp hold-time 60

The above example sets 60 seconds the hold time for vlan 1:

related commands

ip beigrp hello-interval

4.1.16 ip beigrp passive

Syntax

To enable interacting BEIGRP routing update on a certain interface, use the ip beigrp passive command. Use the no form of this command to restore the default value.

ip beigrp passive

no ip beigrp passive

parameter

none

default

The interface is not in passive mode.

Command mode

interface configuration mode

Usage guidelines

If the ip beigrp passive is configured on an interface, then no routing update is received on this interface, and also no neighborhood relation is established between this interface and any accessible neighbors. But a direct route genereate on this interface will be broadcast by other interface that runs the BEIGRP.

example

The following command set vlan 1 as the passive interface:

interface vlan 1

ip beigrp passive

4.1.17 ip beigrp split-horizon

Syntax

To enable Enhanced Interior Gateway Routing Protocol (BEIGRP) split horizon, use the ip beigrp split-horizon command in interface configuration mode. To disable split horizon, use the no form of this command.

ip beigrp split-horizon

no ip beigrp split-horizon

Parameter

none

default

The behavior of this command is enabled by default.

Command mode

interface configuration mode

Usage guidelines

Using this command is to prevent route cycle, so you must confirm that it will not cause any bad effects before turn off the split horizon.

example

interface vlan 1

no ip beigrp split-horizon

The above example disables split horizon on vlan 1:

4.1.18 metric weights

Syntax

To tune Enhanced Interior Gateway Routing Protocol (BEIGRP) metric calculations, use the metric weights command. To reset the values to their defaults, use the no form of this command

metric weight k1 k2 k3 k4 k5

no metric weight

Parameter

parameter	description
k1,k2,k3,k4,k4	Constants that convert an EIGRP metric vector into a scalar quantity.

default

k1: 1

k2: 0

k3: 1

k4: 0

k5: 0

Command mode

router configuration

Usage guidelines

The tuning of the EIGRP metric calculation for a composite metric adopts two steps:

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

Composite metric = K1*BW*256 + K2 * BW/(256 - load) + K3 * DLY * 256,

BW	10Gbps/ bandwidth
DLY	Delay time, 10 milliseconds

If k5 does not equal zero, an additional operation is performed:

Composite metric = Composite metric * K5/(reliability + K4)

K2, K4 and K5 are the left objects of IGRP, compatible with Eigrp protocol of Cisco. In general, Load and Reliability are not used in composite metric algorithm. Therefore, do not change the default value of K2, K4 and K5, unless you confirm that will not cause bad effect, to prevent unexpected result on route decision

example

```
router beigrp 2
network 131.108.0.0 255.255.0.0
metric weights 2 0 2 0 0
```

related commands

bandwidth

delay

4.1.19 Network

Syntax

To specify the network for an Enhanced Interior Gateway Routing Protocol (BEIGRP) routing process, use the network command in routing switch configuration mode. To remove an entry, use the no form of this command.

network *network-number* [*netmask*]

no network *network-number* [*netmask*]

Parameter

parameter	description
network-number	Network address.
netmask	Network mask.

default

none

Command mode

router configuration

Usage guidelines

Various network statements (network commands) can be configured on a routing switch, to enable BEIGRP dynamic routing protocol to run on many networks; use the default mask if there is no configured mask.

example

router beigrp 2
network 131.108.0.0 255.255.0.0
network 122.11.2.0

related commands

router beigrp

4.1.20 Offset

Syntax

To add an offset to incoming and outgoing metrics to routes learned via Enhanced Interior Gateway Routing Protocol (BEIGRP), use the offset command in router configuration mode. To remove an offset list, use the no form of this command.

offset {*type number* **|** *} {**in | out**} *access-list-name offset*

no offset {*type number* **|** *} {**in | out**}

Parameter

parameter	description
In	Applies the access list to incoming metrics.
Out	Applies the access list to outgoing metrics.
access-list-name	Standard access list name to be applied
Offset	Positive offset to be applied to metrics for networks matching the access list.
Type	(Optional) Interface type to which the offset list is applied.
Number	(Optional) Interface number to which the offset list is applied.

default

none

Command mode

router configuration

Usage guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

BEIGRP is a vector metric, so the offset is added to delay

It is recommended to use standard access list when configuring filter list. The configured access list fails if configured with extended access list

example

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 21:

offset * out 21 10

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

offset e0/0 in 21 10

related commands

ip access-list

4.1.21 redistribute

Syntax

To redistribute routes from other routing protocols into the local BEIGRP routing process routing table, use the redistribute command.

redistribute protocol *process* **route-map** *name*

redistribute protocol *process* **[route-map]**

Parameter

parameter	description
protocol	Source protocol from which routes are being redistributed. It must be one of following keywords: bgp, ospf, static , connected, and rip.
process	(Optional) For bgp or bigp, this parameter indicates the 16-digit autonomous number. For OSPF, this parameter indicates the relevant OSPF process ID of the routes need to be redistributed. This marks the rouing process. It is a non-zero decimal number. For rip, there is no need to mark the process.
route-map	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to IS-IS. If not specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported.
name	Name character string of route-map

default

none

Command mode

BEIGRProuter configuration

Usage guidelines

To redistribute direct routes, static routes and routes from other BEIGRP process, the default-metric command is not necessarily to be configured;otherwise, the default-metric must be configueid.

example

default-metric 64 250 255 255 1500
redistribute ospf 1

4.1.22 router beigrp

Syntax

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the router beigrp command in global configuration mode. To delete the BEIGRP routing process, use the no form of this command.

router beigrp *autonomous-system-number [*vrf *vrf-name]*

no router beigrp *autonomous-system-number [*vrf *vrf-name]*

Parameter

parameter	description
autonomous-system-number	Autonomous system number that identifies the routes to the other BEIGRP routers.
vrf-name	Specifies the VRF to which the BEIGRP process belongs.

default

none

Command mode

global configuration mode

Usage guidelines

This command can be used to operate multiple BEIGRP processes.

example

The following example configures EIGRP process 30:

router beigrp 30

related commands

network

4.1.23 show ip beigrp interface

Syntax

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the show ip beigrp interfaces command.

show ip beigrp interfaces [**interface-type** *interface-number* **|** *as-number*]

Parameter

parameter	description
as-number	Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process
interface	Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface

default

none

Command mode

All configuration modes except user mode.

Usage guidelines

Use the show ip eigrp interfaces command to learn information about BEIGRP dynamic routing relating to those interfaces.

related commands

None

4.1.24 show ip beigrp neighbors

Syntax

To display neighbors discovered by Enhanced Interior Gateway Routing Protocol (BEIGRP), use the show ip eigrp neighbors command in EXEC mode.

show ip beigrp neighbors [*interface-type interface-number* **|** *as-number*] [*detail*]

Parameter

parameter	description
as-number	Autonomous system number. If the parameter is specified, it will display only the neighbour of BEIGRP process
interface	Interface name. If the parameter is specified, it will display only the neighbour on this BEIGRP interface
detail	Displays detailed neighbor information.

default

none

Command mode

All configuration modes except user mode.

Usage guidelines

Use the show ip beigrp neighbors command to determine what neighbours they are and when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

example

Router# show ip beigrp neighbors

Information of BEIGRP neighbors with AS 1024

Address interface hold uptime Q_cnt Seq

192.168.20.204 vlan 1 15 00:08:06 0 159

202.117.80.143 vlan 2 10 00:08:05 0 100

192.168.20.141 vlan 1 12 00:07:38 0 254

field	explanation
AS 64	Autonomous system number
Address	IP address of the BEIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time that the software will wait to hear from the peer before declaring it down.
Uptime	Elapsed time since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets that the software is waiting to send.
Seq	Sequence number of the last update that was received from this neighbor.

related commands

None

4.1.25 show ip beigrp protocol

Syntax

To display the Enhanced Interior Gateway Routing Protocol (BEIGRP) routing protocol process parameter and statistics, use the show ip beigrp protocols command.

show ip beigrp protocols [*as-number*]

Parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified, it will display only the parameters and statistics of this BEIGRP process

Command mode

All configuration modes except user mode.

Usage guidelines

This command can be used to check BEIGRP topology table at any time.

example

```
R142#show ip bei pro
Protocol Information of BEIGRP with AS 1024:
 Metric Weight: K1=1, K2=0, K3=1, K4=0, K5=0.
 Filter * in access-list in12
 Filter * out access-list ou12
 Offset * in in23 12
 Offset * out ou23 12
 Redistributing: connect, ospf 1, ospf 2
 Automatic network summarization is enable.
 Active-time: 3(minutes)
 Routing for Networks:
     192.168.20.0/24
 10.0.0.0/8
 167.20.0.0/16
 202.117.80.0/24
 Distance: internal 90, external 170
 Active Route:
```

related commands

None

4.1.26 show ip beigrp topology

Syntax

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the show ip beigrp topology command in privileged EXEC mode.

show ip beigrp topology [[as-number active | all-links | pending | summary | zero-successors] | [network-number subnet-mask]]

Parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified, it will display only the topology table of BEIGRP process
network-number	Displays detailed information about the specified network.
subnet-mask	(Optional) Subnet mask.
active	(Optional) Displays only active entries in the BEIGRP topology table.
all-link	(Optional) Displays all entries in the BEIGRP topology table.
pending	(Optional) Displays all entries in the BEIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the BEIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.

default

none

Command mode

All configuration modes except user mode.

Usage guidelines

This command can be used to check BEIGRP topology table at any time.

example

```
Router# show ip beigrp topology
P 10.10.10.0/24 successors: 1 FD: 13056
 via connect(Loopback1) Metric: 13056/0
    P 167.20.0.0/16 successors: 1 FD: 261132
 via 202.117.80.143(vlan 1) Metric: 261132/258560
    P 192.166.100.0/24 successors: 1 FD: 281856
 via redistribute Metric: 281856/0
    P 192.168.20.0/24 successors: 1 FD: 258560
 via connect(vlan 2) Metric: 258560/0
    P 202.1.1.0/24 successors: 1 FD: 297246988
 via 192.168.20.204(vlan 2) Metric: 297246988/297244416
    P 202.117.80.0/24 successors: 1 FD: 258560
 via connect(vlan 1) Metric: 258560/0
    A 202.117.93.0/24 successors: 1 FD: unaccessible, R serno: 32
 via 192.168.20.141(vlan 2) Metric: 271372/13056
SIA-Info: (active: 00:02:20 query-origin: Local origin)
 Unreplied Neighbors:
 via 202.117.80.143, vlan 1
    P 202.192.168.0/24 successors: 1 FD: 284172
 via 192.168.20.204(vlan 2) Metric: 284172/281600
```

field	description
160.89.90.0 and so on	Destination network number
255.255.255.0	Destination network mask
successors	Number of successors.
FD	Feasible distance.
Via	Gateway address
vlan 2	Interface from which this information was learned.
SIA-Info	active routing information
active	Lasting time when entering Active status.
query-origin	Origin of entering query state
Unreplied Neighbors	Neighbor lists that are not received reply.

related commands

None

4.1.27 show ip beigrp traffic

Syntax

To display the flow information of Enhanced Interior Gateway Routing Protocol (BEIGRP) packets sent and received, use the show ip beigrp traffic command in EXEC mode.

show ip beigrp traffic [*as-number*]

Parameter

parameter	description
as-number	(Optional) Autonomous system number. If the parameter is specified ,then display the flow statistics information

default

none

Command mode

All configuration modes except user mode.

Usage guidelines

Use this command to check the flow statistics information of BEIGRP packets sent and received at any time.

example

R142#show ip bei tra
Traffic Statistics of BEIGRP 1024
Packet Type Hello Update Query Reply ACK
Send/Receive 770/1021 133/44 29/7 7/9 60/147

related commands

None

Chapter 5 OSPF Configuration Commands

5.1 OSPF Configuration Commands

OSPF Configuration Commands Include:

- area authentication
- area default-cost
- area filter
- area nssa
- area nssa-range
- area nssa-translate-interval
- area range
- area stub
- area virtual-link
- auto-cost
- bfd all-interfaces
- debug ip ospf adj
- debug ip ospf events
- debug ip ospf flood
- debug ip ospf lsa-generation
- debug ip ospf packet
- debug ip ospf restart
- debug ip ospf retransmission
- debug ip ospf spf
- debug ip ospf tree
- default-information originate
- default-metric
- distance

- distance ospf
- filter
- graceful-restart
- ip ospf authentication
- ip ospf cost
- ip ospf dead-interval
- ip ospf demand-circuit
- ip ospf hello-interval
- ip ospf message-digest-key
- ip ospf mib-binding
- ip ospf network
- ip ospf passive
- ip ospf password
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- limit max-ext-lsa
- limit retransmissions
- maximum-paths
- neighbor
- network area
- redistribute
- restart ospf
- router-id
- router ospf
- show ip ospf
- show ip ospf border-routers
- show ip ospf database
- show ip ospf interface

- show ip ospf neighbor
- show ip ospf virtual-link
- stub-router
- summary-address
- timers delay-timer
- timers hold-timer
- timers age-timer

5.1.1 area authentication

Syntax

To enable authentication for an Open Shortest Path Firstly (OSPF) area, use the area authentication command in routing switch configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command.

area *area-id* **authentication** {**simple | message-digest**}

no area *area-id* **authentication**

no area *area-id*

Parameter

parameter	description
area-id	Identifier of the area for which authentication is to be enabled.
simple	(Optional)authentication information, Plain text authentication
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument.

Default value

no authentication of interface receiving OSPF packet by default

Command mode

router configuration

Usage guidelines

The authentication value will be added into OSPF packet.The authentication type of all routing swithces in the same area must be the same.The authentication password for all OSPF routing switches on a network must be the same if they are to communicate with each other via OSPF..

Example

The following example mandates authentication simple for areas 0 and 36.0.0.0.

```
interface VLAN1
  ip address 131.119.251.201 255.255.255.0
  ip ospf password 0 adcdefgh
!
interface VLAN2
  ip address 36.56.0.201 255.255.0.0
  ip ospf password 0 ijklmnop
!
router ospf 1
  network 36.0.0.0 255.0.0.0 area 36.0.0.0
  network 131.119.0.0 255.255.0.0 area 0
  area 0 authentication simple
  area 36.0.0.0 authentication simple
!
```

Related commands

ip ospf password

ip ospf message-digest-key

5.1.2 area default-cost

Syntax

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the area default-cost command in router address family topology or routing switch configuration mode. To remove the assigned default route cost, use the no form of this command.

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

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

no area *area-id*

Parameter

parameter	description
area-id	Identifier for the stub area.
cost	Cost for the default summary route used for a stub

Default value

cost.1

Command mode

OSPF Routing configuration mode

Usage guidelines

This command is used only on an routing switch attached to a stub area or NSSA.

After configured the area stub default-information-originate command, the routing switch will send LSA(SUM-NER-LSA) including default router information to correspondent field, the cost configured I this command is the correspondent cost used in LSA.

Note:

To remove the specified area from the software configuration, use the no area area-id command (without other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 area 36.0.0.0 default-cost 20
 area 36.0.0.0 stub
!
```

Related commands

area nssa

area stub

5.1.3 area filter

Syntax

To filter Type-3 LSA of in/out this area, run the following command. To return to the default setting, use the no form of this command.

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

no area *area-id* **filter** {**in | out**}

no area *area-id*

Parameter

Parameter	Description
area-id	Domain which filters Type-3 LSA. It can be a decimal numeral or an ip address.
in	In ABR, filter Type-3 LSA sent to this area.
out	In ABR, filter Type-3 LSA sent from this area to other areas.
access-list-name	Name of access list
prefix-list-name	Name of prefix list

Default value

Disabled

Command mode

OSPF Routing configuration mode

Usage guidelines

The command only works on the ABR, but is not available to the area inner route. In direction **in**, Type-3 LSA of ABR sent to this area does not include the filtered network segment. This rule is also applicable to area-range segment of other areas; in direction **out**, Type-3 LSA of ABR sent to this area does not include the filtered network segment. If all sub-segments covered by an area-range are filtered, the area-range will not generate Type-3 LSA.

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval,area nssa-range, area range, area stub, and area virtual-link.

Example

The following example shows how to configure area 36.0.0.0 which neither receives Type-3 LSA including in 192.0.0.0/8, nor generates Type-3 LSA including in 36.0.0.0/8.

```
!
interface VLAN1
 ip address 192.42.110.201 255.255.255.0
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 network 192.0.0.0 255.0.0.0 area 0
 area 36.0.0.0 filter in prefix-list bd1
 area 36.0.0.0 filter out prefix-list bd2
!
!
ip prefix-list bd1 seq 5 deny 192.0.0.0/8
ip prefix-list bd2 seq 5 deny 36.0.0.0/8
!
```

Related command

area authentication

5.1.4 area nssa

Syntax

To configure a NSSA area, run the following command. To return to the default setting, use the no form of this command.

area *area-id* **nssa** [**default-information-originate [metric** *value* **| metric-type {***1* **|** *2***}] |no-redistribute | no-summary | translate-always**]

no area *area-id* **nssa** [**default-information-originate | no-redistribute | no-summary | translate-always**]

no area *area-id*

Parameter

Parameter	Description
area-id	Area-ID of NSSA. It can be a decimal numeral or an ip address.

default-information-originate	(Optional) For ABR, if this command is configured but without configuring command **no-summany**, whether there is a default route, one Type-7 LSA will be generated to send the default route to the area; if command **no-summany** is configured, a Type-3 LSA will be generated to send the default route to the area. For ASBR, after configuration, only when the main routing table has a default route can Type-7 LSA be generated to sent a default route to the area.
metric	(Optional) default metric
metric-type	(Optional) default metric type of the route
no-redistribute	(Optional) The command is used to diable introduce AS outer route to NSSA by the form of Type-7 LSA. Usually it is only used in ABR of NSSA and ASBR or OSPF.
no-summary	(Optional) The command is only used in ABR of NSSA and disable ABR router forwarding Type-3 LSA to NSSA. After configuration, NSSA ABR send one default route to the area by generating one Type-3 LSA and does not send other Type-3 LSA to the area (The area is also called NSSA Totally Stub).
translate-always	(Optional) Only used for ABR of NSSA domain. ABR works for translating Type-7 LSA into Type-5 LSA.

Default value

Non-NSSA area

Command mode

OSPF Routing configuration mode

Usage guidelines

The command "area nssa" must be configured on all routers and acess servers in NSSA area.

For further decreasing the amount of LSA, use command **no-summary** to sending summarizing LSA to NSSA on ABR.

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval,area nssa-range, area range, area stub, and area virtual-link.

Example

The following example shows how to configure 36.0.0.0 as NSSA area.

```
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
```

```
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 area 36.0.0.0 nssa
 redistribute static
!
```

Related command

area authentication

area default-cost

redistribute

5.1.5 area nssa-range

Syntax

To translate Type-7 LSA for route aggregation, run the following command. To return to the default setting, use the no form of this command.

area *area-id* **nssa-range** *address mask* [**advertise | not-advertise | tag** *value*] [**cost** *cost*] [**cost** cost_value]

no area *area-id* **nssa-range** *address mask*

no area *area-id*

Parameter

Parameter	Description
area-id	Domain of Type-7 LSA route aggregation. It can be a decimal numeral or an ip address.
address	Destination IP address of the aggregation route.
mask	The network mask of aggregation route.
advertise	(Optional) Advertise after aggregation.
not-advertise	(Optional) Not-advertise after aggregation
tag	(Optional) Tag of aggregation route.
value	Route tag. The value ranges from 0 to 4294967295. The default value is 0.
cost	(Optional) Cost of aggregation route
cost_value	Cost value of aggregation route. The value ranges from 0 to 16777215. The default value is the max cost of all aggregated route.

Default value

Disabled

Command mode

OSPF Routing configuration mode.

Usage guidelines

The command can only be configured on the non-trunk domain.

If the local router is ABR and the translation router of NSSA, the command “area nssa-rang” will aggregates Type-7 LSA and generates Type-5 LSA; for translation router not in the NSSA, there is no aggregation.

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval,area nssa-range, area range, area stub, and area virtual-link.

Example

The following example shows how to configure route aggregation of translatable Type-7 LSA in segment 50.0.0.0 of ABR.

```
!
interface VLAN1
 ip address 192.42.110.201 255.255.255.0
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 network 192.0.0.0 255.0.0.0 area 0
 area 36.0.0.0 nssa
 area 36.0.0.0 nssa-range 50.0.0.0 255.0.0.0
!
```

Related command

area nssa

5.1.6 area nssa-translate-interval

Syntax

To configure a time interval a translater elected by Type-7 LSA works after being replaced by another one. To return to the default setting, use the no form of this command.

area *area-id* **nssa-translate-interval** *interval*

no area *area-id* **nssa-translate-interval**

no area *area-id*

Parameter

Parameter	Description
area-id	Area-ID of NSSA. It can be a decimal numeral or an ip address.
interval	Time interval. Unit: s

Default value

40s

Command mode

OSPF Routing configuration mode

Usage guidelines

The command can only be configured on the non-trunk area.

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval, area nssa-range, area range, area stub, and area virtual-link.

Example

The following example shows how to configure the time interval of area 36.0.0.0 to 100s.

```
!
interface VLAN1
 ip address 36.56.0.201 255.255.0.0
```

```
!
router ospf 201
  network 36.0.0.0 255.0.0.0 area 36.0.0.0
  area 36.0.0.0 nssa
  area 36.0.0.0 nssa-translate-interval 100
  redistribute static
!
```

Related command

area nssa

5.1.7 area range

Syntax

To consolidate and summarize routes at an area boundary, use the **area range** command. To disable this function, use the no form of this command.

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

no area *area-id* **range** *address mask*

no area *area-id*

Parameter

parameter	description
area-id	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix.
address	IP address
mask	IP address mask
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Default value

This command is disabled by default.

Command mode

OSPF Routing configuration mode

Usage guidelines

The area range command is used only with Area Border Routing switches. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization.

Multiple area range routing switch configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
!
interface VLAN1
 ip address 192.42.110.201 255.255.255.0
 no ip directed-broadcast
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
 no ip directed-broadcast
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 network 192.0.0.0 255.0.0.0 area 0
 area 0 range 192.42.110.0 255.255.255.0
 area 36.0.0.0 range 36.0.0.0 255.0.0.0
!
```

5.1.8 area stub

Syntax

To define an area as a stub area, use the area stub command. To disable this function, use the no form of this command.

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

no area *area-id* **stub**

no area *area-id*

Parameter

parameter	description
area-id	Identifier for the stub area; either a decimal value or an IP address.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Default value

No stub area is defined.

Command mode

OSPF Routing configuration mode

Usage guidelines

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal route sent into a stub area by an ABR switch.

There are two stub area router configuration commands: the stub and default-cost options of the area routing switch configuration command. In all routing switches attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR switch to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

Example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
```

```
!
!
router ospf 201
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
 area 36.0.0.0 default-cost 20
 area 36.0.0.0 stub
!
```

Related commands

area authentication

area default-cost

5.1.9 area virtual-link

Syntax

To define a virtual link, use the area virtual-link command

area *area-id* **virtual-link** *neighbor-ID* [**authentication** simple | message-digest] [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*][**password** [*0* | *7*] *pass-string*] [**message-digest-key** key-id MD5 [0 | 7] md5-string]

no area area-id **virtual-link** neighbor-ID [authentication] [dead-interval [hello-interval] [retransmit-interval][transmit-delay][password] [message-digest-key key-id]

Parameter

parameter	description
area-id	Area ID assigned to the transit area for the virtual link.
neighbor-id	Router ID associated with the virtual link neighbor.
simple	Plain text authentication. The value must be the same for all routing switches and access servers attached to a common network.
message-digest	Enables Message Digest 5 (MD5) on virtual-link. The value must be the same for all routing switches and access servers attached to a common network.
dead-value	Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The value must be the same for all routing switches and access servers attached to a common network.
hello-value	Time (in seconds) between the hello packets that the software sends on an interface. The value must be the same for all routing switches and access servers attached to a common network.

retrans-value	Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be the same for all routing switches and access servers attached to a common network.
dly-value	Delay value in seconds to inform LSA on virtual-link for a routing switch. The configured value on both sides of the virtual-link should be the same.
pass-string	If virtual-link uses plain text authentication, the the maximum character of the configured password should be 8. The configuied value on both sides of the virtual-link should be the same.
key-id	If virtual-link uses MD5 authentication, the valid range of the used MD5 key should from 1 to 255. The configured value on both sides of the virtual-link should be the same.
MD5-String	Configures MD5 password, which is 16-character at most. The configured value on both sides of the virtual-link should be the same.
0 | 7	Designate the key type: plaintext (0) or ciphertext (7).

Default value

No virtual-link is configured.

Default value of other parameters are as follows:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s, no authentication

Command mode

OSPFrouter configuration

Usage guidelines

To establish a virtual link, user should configure both sides of the virtual link. The virtual link will fail if this command is only configured on one side.

The parameter-id must be a non-zero character, for the virtual link and the transit areda must be a non-backbone area. The configured area-id of the virtual link must be the same.

The neighbor-ID must be the same as the ospf router-id on the remote side during configuration, or the virtual link will not be established. Even if the configured neighbor-ID is another IP address of the other side.

You must make sure that all parameters on both sides must be the same.

The authentication parameters that configured on virtual-link become effective only when configured authentication types of virtual-link or configured the relevant authentication methods in backbone are (via the command area authentication)Only one kind of authentication parameter can be configured on virtual-link, that is, the MD5 and the plain text authenticationm are mutually exclusive.

Use the command no area area-id veitual-link neighbor-ID to cancel the formerly-configured virtual link.

Use the command show ip ospf virtual-link to check state of the virtual link.

Note:

no area area-id (no other parameters)

The command can be used to cancel sub-commands of all domain parameters, such as area authentication, area default-cost, area filter, area nssa, area nssa-translate-interval, area nssa-range, area range, area stub, and area virtual-link.

Example

The following example configured a virtual link between router A and router B:

The configuration on router A (router-id: 200.200.200.1):

```
!
router ospf 100
 network 192.168.20.0 255.255.255.0 area 1
 area 1 virtual-link 200.200.200.2
!
```

The configuration on router B(router-id: 200.200.200.2):

```
!
router ospf 100
 network 192.168.30.0 255.255.255.0 area 1
 area 1 virtual-link 200.200.200.1
!
```

Related commands

show ip ospf virtual-link

5.1.10 auto-cost

Syntax

To configure reference-bandwidth value, run the following command. To return to the default setting, use the no form of this command.

auto-cost reference-bandwidth *value*

no auto-cost reference-bandwidth

Parameter

Parameter	Description
value	Reference-bandwidth value for calculating link cost. The value ranges from 1 to 4294967. Unit: Mbps

Default value

100Mbp

Command mode

OSPF Routing configuration mode

Usage guidelines

If the command is not configured, OSPF calculates cost according to the link bandwidth(cost is equal to bandwidth reference value divided by bandwidth; if the cost is larger than 65535. The max cost is 65535).

If the command is configured, OSPF does not calculate cost based on the link bandwidth, but based on the configured link.

Example

The following example shows how to configure the bandwidth reference of the link to 1000Mbps:

```
!
interface VLAN2
 ip address 36.56.0.201 255.255.0.0
!
router ospf 201
 auto-cost reference-bandwidth 1000
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
!
```

Related command

ip ospf cost

5.1.11 bfd all-interfaces

Syntax

To enable bfd linkage function on all ospf interfaces, use the **bfd all-interfaces** command. To restore the default value, use the **no bfd all-interfaces** command.

bfd all-interfaces

no bfd all-interfaces

Parameter

None

Default

No bfd linkage

Command mode

OSPF Routing configuration mode

Usage guidelines

Configuring bfd all-interfaces will enable the bfd linkage function of all ospf interfaces, except for interfaces configured with the **ip ospf bfd disable** command. Command **bfd all-interfaces** is usually configured when there are many ospf interfaces.

Example

The following example shows how to configure the bfd function of the ospf interface(except for vlan2).

```
interface VLAN1
 ip address 36.56.0.201 255.255.0.0
!
interface VLAN2
 ip address 36.57.0.201 255.255.0.0
 ip ospf bfd disable
!
interface VLAN3
 ip address 36.58.0.201 255.255.0.0
!
router ospf 201
 router-id 1.2.2.1
 network 36.0.0.0 255.0.0.0 area 36.0.0.0
```

bfd all-interfaces
!

Related command

ip ospf bfd

5.1.12 debug ip ospf adj

Syntax

To monitor Open Shortest Path Firstly (OSPF)-related estabilishment process , use the debug ospf adj command

debug ip ospf adj

Parameter

none

Default

none

Command mode

EXEC

Usage guidelines

User can check the process of OSPF-related estabilishment process from the output of this command.

Example

Switch # debug ip ospf adj
OSPF[1]: Interface 0.0.0.0 on VLAN1 going Up
OSPF[1]: 2 Way Communication to 192.85.1.5 on VLAN1, state 2WAY
OSPF[1]: 2 Way Communication to 1.1.1.1 on VLAN1, state 2WAY
OSPF[1]: Interface 0.0.0.0 on VLAN1 Waittmr expired
OSPF[1]: NBR 1.1.1.1 on VLAN1 Adjacency OK, state EXSTART.
OSPF[1]: NBR 192.85.1.5 on VLAN1 Adjacency OK, state EXSTART.
OSPF[1]: NBR 192.85.1.5 Negotiation Done. We are the SLAVE. seq 0x25c83

OSPF[1]: NBR 192.85.1.5 on VLAN1 Negotiation Done. We are the SLAVE

OSPF[1]: Exchange Done with 192.85.1.5 on VLAN1

OSPF[1]: Loading Done with 192.85.1.5 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 192.85.1.5 on VLAN1, database Synchronized (FULL)

OSPF[1]: NBR 192.85.1.4 Negotiation Done. We are the MASTER. seq 0x12b

OSPF[1]: NBR 1.1.1.1 on VLAN1 Negotiation Done. We are the MASTER

OSPF[1]: Exchange Done with 1.1.1.1 on VLAN1

OSPF[1]: Loading Done with 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)

……

5.1.13 debug ip ospf events

Syntax

To monitor OSPF interface and OSPF-related events, , use the debug ip ospf events command.

debug ip ospf events

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF interface and OSPF-related adjacency events from the ouput of this command.

Example

Switch # debug ip ospf events

OSPF: Receive [MSG_OSPF_PROTO_UP] message, index=26

OSPF[1]: Interface VLAN1 going Up

OSPF: INTF(192.85.1.0) event INTF_UP

OSPF[1]: Interface 192.85.1.0 on VLAN1 going Up
OSPF: Receive [MSG_OSPF_TASKPOLICY_CHANGE] message
OSPF: NBR(192.85.1.5) event HELLO_RX
OSPF: NBR(192.85.1.4) event HELLO_RX
OSPF: NBR(192.85.1.4) event TWOWAY
OSPF[1]: 2 Way Communication to 1.1.1.1 on VLAN1, state 2WAY
OSPF: NBR(192.85.1.5) event TWOWAY
OSPF[1]: 2 Way Communication to 192.85.1.5 on VLAN1, state 2WAY
OSPF: INTF(192.85.1.0) event WAIT_TIMER
OSPF[1]: Interface 192.85.1.0 on VLAN1 Waittmr expired
OSPF: NBR(192.85.1.4) event ADJ_OK
OSPF[1]: NBR 1.1.1.1 on VLAN1 Adjacency OK, state EXSTART.
OSPF: NBR(192.85.1.5) event ADJ_OK
OSPF[1]: NBR 192.85.1.5 on VLAN1 Adjacency OK, state EXSTART.
OSPF[1]: NBR 192.85.1.4 Negotiation Done. We are the MASTER. seq 0x3a1
OSPF: NBR(192.85.1.4) event NEGO_DONE
OSPF[1]: NBR 1.1.1.1 on VLAN1 Negotiation Done. We are the MASTER
OSPF: NBR(192.85.1.4) event EXCH_DONE
OSPF[1]: Exchange Done with 1.1.1.1 on VLAN1
OSPF: NBR(192.85.1.4) event LOAD_DONE
OSPF[1]: Loading Done with 1.1.1.1 on VLAN1, database Synchronized (FULL)
OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)
OSPF[1]: NBR 192.85.1.5 Negotiation Done. We are the SLAVE. seq 0x25efb
OSPF: NBR(192.85.1.5) event NEGO_DONE
OSPF[1]: NBR 192.85.1.5 on VLAN1 Negotiation Done. We are the SLAVE
OSPF: NBR(192.85.1.5) event EXCH_DONE
OSPF[1]: Exchange Done with 192.85.1.5 on VLAN1
OSPF: NBR(192.85.1.5) event LOAD_DONE
OSPF[1]: Loading Done with 192.85.1.5 on VLAN1, database Synchronized (FULL)
OSPF[1]: Loading Done with Nbr 192.85.1.5 on VLAN1, database Synchronized (FULL)
……

5.1.14 debug ip ospf flood

Syntax

To display OSPF-related database pervasion process, use the debug ip ospf flood command.

debug ip ospf flood

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF-related database pervasion process from the output of this command.

Example

Switch # debug ip ospf flood

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 15 SEQ 0x80000004 in area 0

OSPF[1]: not_my_lsa new DB(192.85.1.5) type 1 AGE 15 SEQ 0x80000004 CHKS 0x2d94

OSPF[1]: recv UPDATE, type 1 LSID 1.1.1.1 ADV_RTR 1.1.1.1 AGE 15 SEQ 0x80000003 in area 0

OSPF[1]: not_my_lsa new DB(1.1.1.1) type 1 AGE 15 SEQ 0x80000003 CHKS 0x7281

OSPF[1]: recv UPDATE, type 2 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 20 SEQ 0x80000001 in area 0

OSPF[1]: not_my_lsa new DB(192.85.1.5) type 2 AGE 20 SEQ 0x80000001 CHKS 0x7d66

OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: Loading Done with Nbr 192.85.1.5 on VLAN1, database Synchronized (FULL)

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 8 SEQ 0x80000002 in area 0

OSPF[1]: when add DB(192.85.1.1) type 1, we fount it

OSPF[1]: recv self originate DB(192.85.1.1) type 1, same instance

OSPF[1]: recv UPDATE, type 2 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 1 SEQ 0x80000002 in area 0

OSPF[1]: when add DB(192.85.1.5) type 2, we fount it

OSPF[1]: not_my_lsa MORE_RECENT DB(192.85.1.5) type 2 AGE 20 SEQ 0x80000001 CHKS 0x7d66

OSPF[1]: Send UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 1 SEQ 0x80000003 in the area 0

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 2 SEQ 0x80000003 in area 0

OSPF[1]: when add DB(192.85.1.1) type 1, we fount it

OSPF[1]: recv self originate DB(192.85.1.1) type 1, same instance

OSPF[1]: recv UPDATE, type 2 LSID 192.85.1.5 ADV_RTR 192.85.1.5 AGE 1 SEQ 0x80000003 in area 0

OSPF[1]: when add DB(192.85.1.5) type 2, we fount it

OSPF[1]: not_my_lsa MORE_RECENT DB(192.85.1.5) type 2 AGE 1 SEQ 0x80000002 CHKS 0xf6cf

……

5.1.15 debug ip ospf lsa-generation

Syntax

To display OSPF-related LSA generation process, use the debug ip ospf lsa generation command.

debug ip ospf lsa-generation

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF interface and adjacency events from the output of this command.

Example

router# debug ip ospf lsa-generation

……

OSPF[1]: addLSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: add new LSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: Build RTR_LSA for area 0, rID 192.85.1.1, seq0x80000001

OSPF[1]: addLSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: find the same LSA, type:1, ls_id:192.85.1.1, adv_rtr:192.85.1.1, in area 0

OSPF[1]: Build RTR_LSA for area 0, rID 192.85.1.1, seq0x80000002

OSPF[1]: addLSA, type:1, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0

OSPF[1]: add new LSA, type:1, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0

OSPF[1]: addLSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0

OSPF[1]: add new LSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0

OSPF[1]: addLSA, type:2, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0

OSPF[1]: add new LSA, type:2, ls_id:192.85.1.5, adv_rtr:192.85.1.5, in area 0
OSPF[1]: Loading Done with Nbr 1.1.1.1 on VLAN1, database Synchronized (FULL)

OSPF[1]: addLSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0

OSPF[1]: find the same LSA, type:1, ls_id:1.1.1.1, adv_rtr:1.1.1.1, in area 0
……

5.1.16 debug ip ospf packet

Syntax

To display OSPF packets, use the debug ip ospf packet command.

debug ip ospf packet [ack | dd | hello | update | request]

Parameter

Parameter	Description
ack	Monitors OSPF ACK packets.
dd	Monitors OSPF DD packets.
hello	Monitors OSPF Hello packets.
update	Monitors OSPF Update packets.
request	Monitors OSPF Request packets.

Default value

none

Command mode

EXEC

Usage guidelines

To display OSPF interface and adjacency events from the output of this command.

Example

Switch# debug ip ospf packet

OSPF: Recv a packet from source: 192.85.1.4 dest 224.0.0.5

OSPF[1]: Recv HELLO from 1.1.1.1(addr: 192.85.1.4) area 0 from VLAN1

OSPF[1]: End of hello processing

OSPF: Recv IP_SOCKET_RECV_PACKET message, length=72

OSPF: Recv a packet from source: 192.85.1.5 dest 224.0.0.5

OSPF[1]: Recv HELLO from 192.85.1.5(addr: 192.85.1.5) area 0 from VLAN1

OSPF[1]: End of hello processing

OSPF[1]: Send HELLO to 224.0.0.5 on VLAN1. HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 52

OSPF: Recv IP_SOCKET_RECV_PACKET message, length=72

OSPF: Recv a packet from source: 192.85.1.4 dest 224.0.0.5

OSPF[1]: Recv HELLO from 1.1.1.1(addr: 192.85.1.4) area 0 from VLAN1

OSPF[1]: End of hello processing

……

OSPF: Recv a packet from source: 192.85.1.5 dest 224.0.0.5

OSPF[1]: recv UPDATE packet from 192.85.1.5 (addr: 192.85.1.5) area 0 from VLAN1 len 64 advcnt 1

OSPF[1]: recv UPDATE, type 1 LSID 192.85.1.1 ADV_RTR 192.85.1.1 AGE 7 SEQ 0x80000002 in area 0

OSPF[1]: Send ACK, type 1, LSID 192.85.1.1, ADV_RTR 192.85.1.1, AGE 5, SEQ 0x80000002

OSPF[1]: Send ACK to 192.85.1.5(RID 192.85.1.5) len 44 on VLAN1

……

5.1.17 debug ip ospf restart

Syntax

To moniter the smooth restart process of OSPF, run the following command.

debug ip ospf restart

Parameter

None

Default value

None

Command mode

Exec

Usage guidelines

The command is used to output information and show the smooth restart process of OSPF.

Example

GR Restarter end:

Switch# debug ip ospf restart

OSPF: Recv MSG_OSPF_GRACEFUL_RESTART message

OSPF: Build grace-LSA, adv_rtr:5.5.5.5, in area 0, at interface VLink 0.0.0.0

OSPF: Build grace-LSA, adv_rtr:5.5.5.5, in area 1, at interface VLAN1

OSPF: grace-LSAs have been flooded out. switch redundant

OSPF: The OSPF process 1 is restarting gracefully now.

OSPF: Recv MSG_OSPF_RESTART message

OSPF: OSPF process 1 is restarting

OSPF: Database resynchronized with 12.12.12.12 on VLAN1 done, to FULL

OSPF: OSPF process 1 has reestablished all its adjacencies. GR successfully

OSPF: Recv MSG_OSPF_GR_TERMINATE message

OSPF: GR of OSPF process 1 terminated

GR Helper end:

router# debug ip ospf restart

OSPF: IETF GR Received grace-LSA from 5.5.5.5(addr: 192.167.1.1) on VLink 192.167.1.1

OSPF: IETF GR Validate grace-LSA from nbr 5.5.5.5 on VLink 192.167.1.1

OSPF: IETF GR Process grace-LSA from nbr 5.5.5.5 on VLink 192.167.1.1, age 1, grace period 200, graceful restart reason: Switch to redundant control processor, graceful ip address: 0.0.0.0

OSPF: IETF GR Enter graceful restart helper mode for nbr 5.5.5.5 on VLink 192.167.1.1 for 199 seconds (requested 200 sec)

OSPF: IETF GR Received grace-LSA from 5.5.5.5(addr: 192.167.1.1) on FastEthernet0/0

OSPF: IETF GR Validate grace-LSA from nbr 5.5.5.5 on FastEthernet0/0

OSPF: IETF GR Process grace-LSA from nbr 5.5.5.5 on FastEthernet0/0, age 1, grace period 200, graceful restart reason: Switch to redundant control processor, graceful ip address: 192.167.1.1

OSPF: IETF GR Enter graceful restart helper mode for nbr 5.5.5.5 on FastEthernet0/0 for 199 seconds (requested 200 sec)

OSPF: IETF GR Resynchronize with nbr 5.5.5.5(addr: 192.167.1.1)

OSPF: IETF GR Received grace-LSA from 5.5.5.5(addr: 192.167.1.1) on FastEthernet0/0

```
OSPF: IETF GR Validate grace-LSA from nbr 5.5.5.5 on FastEthernet0/0
```

OSPF: IETF GR Process grace-LSA from nbr 5.5.5.5 on FastEthernet0/0, age 3600, grace period 200, graceful restart reason: Switch to redundant control processor, graceful ip address: 192.167.1.1

```
OSPF: Recv MSG_OSPF_GR_HELP_RT_TERMINATE message
```

OSPF: IETF GR Exiting graceful restart helper mode for nbr 5.5.5.5(addr: 192.167.1.1) on VLink 192.167.1.1 with 21 secs remaining

```
OSPF: scheduling rtr lsa for area 0 process 1
```

OSPF: IETF GR Exiting graceful restart helper mode for nbr 5.5.5.5(addr: 192.167.1.1) on FastEthernet0/0 with 21 secs remaining

OSPF: scheduling rtr lsa for area 1 process 1

OSPF: scheduling net lsa on intf FastEthernet0/0

5.1.18 debug ip ospf retransmission

Syntax

To display retransmission of OSPF paceket, uset the debug ip ospf retransmission command;

debug ip ospf retransmission

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display transmission processo OSPF packets.

Example

Switch# debug ip ospf retransmission

OSPF: retransmit UPDATE to 192.168.40.3 (RID 192.168.40.3), state FULL

……

5.1.19 debug ip ospf spf

Syntax

To display information of SPF algorithm, use the following commands.

debug ip ospf spf

debug ip ospf spf intra

debug ip ospf spf inter

debug ip ospf spf external

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

The debug ip ospf spf statistic command displays the OSPF routes calculation process.

Example

Switch # debug ip ospf spf

OSPF[1]: too soon to run SPF, or SPF already scheduled.

OSPF[1]: run ospf_spf_run for area 0

OSPF[1]: start doing SPF for AREA 0, RTAB_REV(ospf) 2.

OSPF: Initializing to do SPF

OSPF[1]: SPF Area 0 running Router LSA

OSPF[1]: ospf_nh_find: 192.85.1.1

OSPF[1]: Area(0) add LSA(192.85.1.5, LS_NET) 1 under LSA(192.85.1.1, LS_RTR)

OSPF: ospf_rtr_netbacklink is called

OSPF[1]: ospf_nh_add 192.85.1.5

OSPF[1]: Area(0) add LSA(192.85.1.5, LS_RTR) 1 under LSA(192.85.1.5, LS_NET)

OSPF: ospf_rtr_netbacklink is called

OSPF[1]: ospf_nh_add 192.85.1.4

……

OSPF[1]: ospf_update_local_table, DEST 192.85.1.0, MASK 255.255.255.0, OSPF_REV 2, calc in area 0, AREA_REV 2

OSPF[1]: info REV 1, LS_TYPE 0, redorded in area 0, AREA_REV 2, state 12

OSPF[1]: info REV 2, LS_TYPE 2, redorded in area 0, AREA_REV 2, state 1

OSPF[1]: end doing SPF for AREA 0

OSPF[1]: finish ospf_spf_run for area 0 with err_code 0

OSPF[1]: ospf_add_main_table

OSPF[1]: delete route 192.85.1.0 first (255.255.255.0).

OSPF[1]: ospf_create_main_table_route equi_lsdb_num=1 maximum_paths=8

OSPF[1]: ospf_create_main_table_route RT 192.85.1.0 LS_TYPE 2 nh 192.85.1.1 area 0.0.0.0

OSPF[1]: build route 192.85.1.0/24 nh num=1, state=0x00031000.

Description of the displaying fields:

Field	Description
LSA(192.85.1.5, LS_NET)	ID and type of LSA

5.1.20 debug ip ospf tree

Syntax

To display establishment of SPF tree of OSPF, use the debug ip ospf tree.

debug ip ospf tree

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display establishment of SPF tree of OSPF from the output of this command.

Example

Switch # debug ip ospf tree

OSPF[1]: Area(0) add LSA(192.85.1.1, LS_NET) 1 under LSA(192.85.1.1, LS_RTR)
OSPF[1]: Area(0) add LSA(1.1.1.1, LS_RTR) 1 under LSA(192.85.1.1, LS_NET)
OSPF[1]: Area(0) add LSA(192.85.1.5, LS_RTR) 1 under LSA(192.85.1.1, LS_NET)
OSPF[1]: Area(0) add LSA(1.0.4.1, LS_SUM_NET) 2 under LSA(1.1.1.1, LS_RTR)
OSPF[1]: Area(0) add LSA(56.0.0.1, LS_SUM_NET) 2 under LSA(1.1.1.1, LS_RTR)
OSPF[1]: Area(0) add LSA(11.1.1.1, LS_SUM_NET) 2 under LSA(1.1.1.1, LS_RTR)

OSPF[1]: call ospf_update_local_table_BFS

Description of the displaying fields:

Field	Description
LSA(1.0.4.1, LS_SUM_NET)	ID and type of LSA
add	Sub-LSA
under	parent LSA

5.1.21 default-information originate

Syntax

To generate a default route into an Open Shortest Path Firstly (OSPF) routing domain, use the **default-information originate** command

default-information originate [**always | metric-type** [*1* | *2*] **| metric** *cost* **| route-map** *map-name*]

no default-information originate

Parameter

parameter	description
originate	Generate a default external route into an Open Shortest Path Firstly (OSPF) routing domain
Always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric-type [*1* | *2*]	(Optional) Metric value type. The value ranges from 1 to 2. The default value is 2.
metric *cost*	(Optional) The routing cost value ranges from 0 to 16777214, and the default value is 100.
route-map map-name	(Optional) Routing process will generate the default route if the route map is satisfied.

Default value

This command is disabled by default.

Command mode

router configuration

Usage guidelines

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPF routing domain, the software automatically becomes an Autonomous System Boundary Router Switch. However, an ASBR Switch does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the always keyword.

When you use this command for the OSPF process, you must satisfy the route-map argument. Use the **default-information originate always route-map** command when you do not want the dependency on the default network in the routing table.

Example

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
!
router ospf 109
 default-information originate metric-type 1
 redistribute rip 1
!
```

Related commands

Redistribute

5.1.22 default-metric

Syntax

To set default metric values for the Open Shortest Path Firstly (OSPF) routing protocol, use the default-metric command. To return to the default state, use the no form of this command.

default-metric *value*

no default-metric

Parameter

parameter	description
value	Default metric value appropriate for the specified routing protocol, in the range 1~16777214.

Default value

Default metric value is 10.

Command mode

OSPF Routing configuration mode

Usage guidelines

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Example

The example assigns 3 as the default metric routes.

Switch_config_ospf_100#default-metric 3

Related commands

redistribute

5.1.23 distance

Syntax

To set the management distance based on the router-id of inform route and of ospf route set by the destination segment, run the following command. To return to the default setting, use the no form of this command.

distance *value* [*network mask] [access-list-name]*

no distance *value* [*network mask]*

Parameter

Parameter	Description
value	(Optional) management distance. The value ranges from 1 to 255.
network	(Optional) The segment which router-id of the inform router locates
mask	(Optional) The segment mask which router-id of the inform router locates
access-list-name	(Optional) Name of the access list

Default value

intra-area: 110

inter-area: 110

external: 150

Command mode

OSPF Routing configuration mode

Usage guidelines

At least there is a parameter.

The command works the same with command “distance ospf”. While this command can set a finer management distance according to router-id of the inform router and destination segment.

Example

The following example shows how to set the management distance of the route complying with the list bd which sent by router 1.1.1.1. as 100:

```
!
router ospf 1
  distance 100 1.1.1.1 255.255.255.255 bd
  redistribute ospf 2
!
```

Related command

distance ospf

5.1.24 distance ospf

Syntax

To define Open Shortest Path Firstly (OSPF) route administrative distances based on route type, use the distance ospf command To restore the default value, use the no form of this command.

distance ospf {[**intra-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}

no distance ospf [**intra-area**] [**inter-area**] [**external**]

Parameter

parameter	description
intra-area dist1	(Optional) Sets the distance for routes in an area, learned by redistribution. The default value is 110.
inter-area dist2	(Optional) Sets the distance for all routes from one area to another area. The default value is 110.
external dist3	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 150.

Default value

intra-area: 110

inter-area: 110

external: 150

Command mode

OSPF Routing configuration mode

Usage guidelines

There is at least one parameter.

This command performs the same function as the distance command used with an access list. However, the distance ospf command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

Example

The following example changes the external distance to 200:

```
Switch A:
!
```

```
router ospf 1
 distance ospf external 200
 redistribute ospf 2
!
router ospf 2
 distance ospf external 200
 redistribute ospf 1
!
Switch B:
!
router ospf 1
 distance ospf external 200
 redistribute ospf 2
!
router ospf 2
 distance ospf external 200
 redistribute ospf 1
!
```

Related commands

distance

5.1.25 filter

Syntax

To configure routing fliter list, use the **filter** command. Use the no filter command to restore the default.

filter {**interface-type** *interface*-number **|** *****} **in** {**access-list** *access-list-name* **|** **gateway** *access-list-name* **|** **prefix-list** *prefix-list-name*}

no filter {**interface-type** *interface*-number **|** *****} **in**

Parameter

parameter	description
***interface*-type**	Interface type
interface-number	Interface number
*****	All interfaces
In	Filters incoming ospf routes
access-list-name	Name of access list

access-list-name	Name of access list
prefix-list-name	Name of prefix list

Default value

none

Command mode

OSPF Routing configuration mode

Usage guidelines

none

Example

Switch_config_ospf_1#filter * in access-list mylist

5.1.26 graceful-restart

Syntax

To set OSPF graceful restart and related parameters, run the following command. To return to the default setting, use the no form of this command.

graceful-restart { **ietf [helper {disable | strict-lsa-checking }] | interval** *period* }

no graceful-restart { **ietf [helper {disable | strict-lsa-checking }] | interval** }

Parameter

Parameter	Description
ietf	Enables graceful restart of IETF standard (based on rfc 3623). The command is disabled by default.
interval *period*	Configures the time limit of graceful restart. The value ranges from 40~1800s. The default value is 120s.
helper disable	(Optional) Disable GR helper. By default, the device can be GR helper of any OSPF neighbor.
helper strict-lsa-checking	(Optional) Enable strict-lsa-checking. When GR Helper detects the change of LSA, exit from Help mode. The command is disabled by default.

Default value

None

Command mode.

OSPF Routing configuration mode

Usage guidelines

None

Example

```
!
router ospf 1
 router-id 192.85.1.1
 network 192.85.1.0 255.255.255.0 area 0
 graceful-restart ietf
 graceful-restart interval 90
!
```

5.1.27 ip ospf authentication

Syntax

To designate the authentication mode of an interface receiving and sending ospf packets, run the following command. To return to the default setting, use the no form of this command.

ip ospf authentication { **simple | message-digest** }

no ip ospf authentication

Parameter

Parameter	Description
simple	Authentication information verified by the plaintext
message-digest	Authentication information verified by MD5

Default value

No authentication

Command mode

Interface configuration mode

Usage guidelines

If use the command "**ip ospf authentication simple**" to verify the interface with the plaintext, you must configure a plaintext password with the command "**ip ospf password**". If use the command "**ip ospf authentication message-digest**" to designate the specified interface with md5 encryption authentication, you must configure md5 key with the command "**ip ospf message-digest-key**". If in one network, all OSPF are guaranteed with OSPF mutual communication, they must share the same verification type and passwords.

Considering the compatibility, the authentication type of one ospf domain must be kept. If no ospf authentication type is configured on the interface, the authentication type of the domain which the interface belongs to will be used (The default authentication type is no authentication.)

Example

The following example shows how to verify interface VLAN 2 with md5 verification.

```
!
interface VLAN2
 ip address 131.119.251.201 255.255.255.0
 no ip directed-broadcast
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 abcdefg
!
router ospf 1
 network 131.119.0.0 255.255.0.0 area 0
!
```

Related command

ip ospf password

ip ospf message-digest-key

area authentication

5.1.28 ip ospf bfd

Syntax

To enable BFD fast check function in the routing configuration mode, run the following command.

ip ospf bfd

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

ip ospf bfd [disable]

To disable interface bfd, run the following command.

no ip ospf bfd

Parameter

disable: disable the function of bfd on the interface

Default value

No bfd

Command mode

Interface configuration mode

Usage guidelines

This function enables ospf and bfd collaborating to detect change of the fast detection link status.

Example

The following example shows how to enable bfd collaboration on the interface vlan2:

```
!
interface VLAN2
 ip address 172.16.0.1 255.255.0.0
 no ip directed-broadcast
 ip ospf bfd
!
router ospf 110
 network 172.16.0.0 255.255.0.0 area 1
!
```

Related command

bfd all-interfaces

5.1.29 ip ospf cost

Syntax

To specify the cost of OSPF protocol on an interface, use the ip ospf cost command in interface configuration mode. To restore to the default value, use the no form of this command.

ip ospf cost *cost*

no ip ospf cost

Parameter

parameter	description
cost	the cost of OSPF protocol. It can be a value in the range from 1 to 65535.

Default value

Default value of the OSPF protocol cost depends on rate of the interface.

Command mode

interface configuration mode

Example

The following example sets the interface cost value to 2:

Switch_config_v2#ip ospf cost 2

specify the the interface cost of OSPF protocol, to restore the default value,use the no ip ospf command.

5.1.30 ip ospf dead-interval

Syntax

To set the dead-interval of specified routing switch in neighbourhood, use the ip ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameter

parameter	description
Seconds	Interval (in seconds) of specified routing switch in neighbourhood. The range is 1 to 2147483647.

Default value

40 seconds

Command mode

interface configuration

Usage guidelines

The dead interval is advertised in OSPF hello packets and sent with OSPF hello packets. This value must be the same for all networking devices on a specific network and four times the interval set by the ip ospf hello-interval command.

Example

The following example sets the OSPF dead interval to 60 seconds:

```
Switch_config_v2#ip ospf dead-interval 60
```

Related commands

ip ospf hello-interval

5.1.31 ip ospf demand-circuit

Syntax

To designate the interface as the demand circuit, run the following command. To return to the default setting, use the no form of this command.

ip ospf demand-circuit

no ip ospf demand-circuit

Parameter

None

Default value

Disabled

Command mode

Interface configuration mode

Usage guidelines

After configuring the on-demand circuit, hello packets and periodically link status update packets can be suppressed. The bottom link can be disabled after the network topology is stable.

Example

The following example shows how to configure interface VLAN2 as on-demand circuit.

Switch_config_v2#ip ospf demand-circuit

5.1.32 ip ospf hello-interval

Syntax

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the ip ospf hello-interval command. To return to the default value, use the no form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter

parameter	description
Seconds	Specifies the interval (in seconds)of sending hello packets. The range is from 1 to 65535.

Default value

10 seconds

Command mode

interface configuration mode

Usage guidelines

This value is advertised in the hello packets and sent with the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Example

The following example sets the interval between hello packets to 20 seconds:

```
Switch_config_v2#ip ospf hello-interval 20
```

Related commands

ip ospf dead-interval

5.1.33 ip ospf message-digest-key

Syntax

To enable Open Shortest Path Firstly (OSPF) Message Digest 5 (MD5) authentication, use the ip ospf message-digest-key md5 command. To remove an old MD5 key, use the no form of this command.

ip ospf message-digest-key *keyid* **md5** [*0* | *7*] *key*

no ip ospf message-digest-key [*keyid*]

Parameter

parameter	description
keyid	An identifier in the range from 1 to 255.
key	Alphanumeric password of up to 16 bytes.
0 | *7*	Designate the key type: plaintext (0) or ciphertext (7)

Default value

OSPF MD5 authentication is disabled.

Command mode

interface configuration mode

Usage guidelines

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

```
!
interface VLAN2
  no ip address
  no ip directed-broadcast
  ip ospf message-digest-key 100 md5 0 OLD
!
```

You change the configuration to the following:

```
!
interface VLAN2
  no ip address
  no ip directed-broadcast
  ip ospf message-digest-key 100 md5 0 OLD
  ip ospf message-digest-key 101 md5 NEW
!
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet - he first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface VLAN2
no ip ospf message-digest-key 100
```

Then, only key 101 is used for authentication on Ethernet VLAN2.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

Example

The following example sets a new key 19 with the password 8ry4222:

```
!
interface VLAN2
 ip ospf message-digest-key 10 md5 0 xvv560qle
 ip ospf message-digest-key 19 md5 0 8ry4222
 !
```

Related commands

area authentication

5.1.34 ip ospf mib-binding

Syntax

To set OSPF progress of mib, run the following command. To return to the default setting, use the no form of this command.

ip ospf mib-binding *process-id*

no ip ospf mib-binding

Parameter

Parameter	Description
process-id	OSPF process ID. The value ranges from 1 to 65535.

Default value

MIB operation binds on OSPF with the most small progress.

Command mode

Global configuration mode.

Usage guidelines

When multiple OSPF progresses are configured, the command can be used to bind MIB with a specific OSPF progress.

Example

The following example shows how to bind MIB operation to OSPF 100:

Switch_config#ip ospf mib-binding 100

5.1.35 ip ospf network

Syntax

To configure the Open Shortest Path Firstly (OSPF) network type, use the ip ospf network command. To return to the default value, use the no form of this command.

ip ospf network { **broadcast | non-broadcast | point_to_multipoint** [**broadcast | non-broadcast**]| **point-to-point**}

no ip ospf network

Parameter

parameter	description
broadcast	Sets the network type to broadcast.
nonbroadcast	Sets the network type to nonbroadcast multiaccess
point-to-point	Sets the network type to point-to-point.
point-to-multipoint	Sets the network type to point-to-multipoint.

Command mode

interface configuration mode

Usage guidelines

Using this feature, you can configure broadcast networks as NBMA networks. Configuring NBMA networks as point-to-multipoint network if there is no assurance to direct connection between any two routing switches..

Example

The following example sets VLAN2 as a nonbroadcast network type:

Switch_config_v2#ip ospf network non-broadcast

5.1.36 ip ospf passive

Syntax

To cancel sending a HELLO packets on an interface, use the ip ospf passive command. Use the no form of this command to reactivate the sending of HELLO packet.

ip ospf passive

no ip ospf passive

Parameter

This command has no keywords or parameters.

Default value

Send HELLO packets on the interface.

Command mode

interface configruration mode

Usage guidelines

If you cancel sending a HELLO packet on an interface, a specified subnetwork wll keep on declaring to other interfaces, and the routing update from other routing switch to this interface can still be received and dealt with. This is usually applicable to the STUB network, for in this kind of network there is usually no other OSPF routing switches.

Example

The following example sends a HELLO packet to all interfaces(except for VLAN2) overridden by network 172.16.0.0:

```
!
interface VLAN2
 ip address 172.16.0.1 255.255.0.0
 no ip directed-broadcast
 ip ospf passive
!
router ospf 110
 network 172.16.0.0 255.255.0.0 area 1
!
```

Related commands

None

5.1.37 ip ospf password

Syntax

To configure password for a neighbor route, use the ip ospf password command. Use the no form of this command to cancel the configuration.

ip ospf password [*0* **|** *7*] *password*

no ip ospf password

Parameter

parameter	description
password	Any consecutive 8-digit character string
0 | 7	Designate the key type: plaintext (0) or ciphertext (7).

Default value

No password is predefined by default.

Command mode

Interface configuration mode

Usage guidelines

The password generated by this command directly inserts OSPF information packet. This command can configure one password for each network of each interface. All neighbor routers must have the same password to exchange OSPD routing information.

When the configured key is displayed, it will be displayed as plain text or cipher text according to the global command.

Example

ip ospf password *yourpsw*

Related commands

area authentication

5.1.38 ip ospf priority

Syntax

To set the router priority, use the ip ospf priority command. To return to the default value, use the no form of this command.

ip ospf priority *priority*

no ip ospf priority

Parameter

parameter	description
priority	specifies the priority. The range is from 0 to 255.

Default value

Priority of 1

Command mode

interface configuration mode

Usage guidelines

When two routing switches attached to a network both attempt to become the designated routing switch, the one with the higher routing switch priority takes precedence. If there is a tie, the routing switch with the higher routing switch ID takes precedence. A routing switch with a routing switch priority set to zero is ineligible to become the designated routing switch or backup designated routing switch. routing switch priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

Example

The following example sets the routing switch priority value of VLAN2 to 8:

Switch_config_v2#ip ospf priority 8

Related commands

neighbor

5.1.39 ip ospf retransmit-interval

Syntax

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the ip ospf retransmit-interval command. To return to the default value, use the no form of this command.

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Parameter

parameter	description
seconds	Time (in seconds) between retransmissions. The range is from 1 to 3600 seconds.

Default value

The default is 5 seconds.

Command mode

interface configuration mode

Usage guidelines

When a routing switch sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the routing switch receives no acknowledgment, it will resend the LSA. The setting of the seconds argument should be greater than the expected round-trip delay between any two routing switches on the attached network..

Example

The following example sets the retransmit interval value to 8 seconds:

Switch_config_v2#ip ospf retransmit-interval 8

5.1.40 ip ospf transmit-delay

Syntax

To set ip ospf transmit-delay time on the interface, run the following command. To return to the default setting, use the no form of this command.

ip ospf transmit-delay *time*

no ip ospf transmit-delay

Parameter

Parameter	Description
time	ip ospf transmit-delay time Unit:s, the value ranges from 1 to 3600.

Default value

1s

Command mode

Interface configuration mode

Example

The following example shows how to configure the transmit-delay time on interface VLAN2 as 3s.

Switch_config_v2#ip ospf transmit-delay 3

5.1.41 ip ospf mtu-ignore

Syntax

To set the port to not check the mtu value in the message, use **ip ospf mtu-ignor** command. Use no form of the command to restore the default settings.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Default

The default state of the interface is to check the mtu value in the packet.

Command mode

Interface configuration mode

Example

The following example shows how to configure not to check the mtu value on interface VLAN2.

Switch_config_v2#ip ospf mtu-ignore

5.1.42 limit max-ext-lsa

Syntax

To set max amount of AS external LSA, run the following command. To return to the default setting, use the no form of this command.

limit max-ext-lsa *value*

no limit max-ext-lsa

Parameter

Parameter	Description
value	Max amount of AS external LSA. The value ranges from 0 to 1000000.

Default value

No limit to the max amount of AS external LSA.

Command mode

OSPF Routing configuration mode.

Usage guidelines

The command is used to set all routes in OSPF autonomous domain as the same value.

Example

To set max amount of AS external LSA in OSPF progress 100 to be 1000:

Switch_config#router ospf 100

Switch_config _ospf_100#limit max-ext-lsa 1000

5.1.43 limit retransmissions

Syntax

To set the max re-transmit times of ospf, run the following command. The re-transmit packets are DD, REQ and LSU. To return to the default setting, use the no form of this command.

limit retransmissions { *timers* **| disable }**

no limit retransmissions [dsiable]

Parameter

Parameter	Description
timers	Max re-transmit times (The default value is 25)
disable	Cancel the max re-transmit times (No limit to the re-transmit)

Default value

The default re-transmit times is 25.

Command mode

OSPF Routing configuration mode

Usage guidelines

None

Example

The following example shows how to modify the retransmit times to 10:

Switch_config_ospf_100#limit retransmissions 10

The following example shows how to restart the retransmit times without limit:

Switch_config_ospf_100#limit retransmissions disable

5.1.44 maximum-paths

Syntax

To set the max amount of next hop of the equivalent route, run the following command. To return to the default setting, use the no form of this command.

maximum-paths *value*

no maximum-paths

Parameter

Parameter	Description
value	The max amount of next hop of the equivalent route. The value ranges from 1 to 8.

Default value

8

Command mode

OSPF Routing configuration mode

Usage guidelines

If the value is 1, the load distribution does not work.

Example

The following example shows how to set next hop of the equivalent route in OSPF progress 100 to be 3.

Switch_config#router ospf 100

Switch_config_ospf_100#maximum-paths 3

5.1.45 neighbor

Syntax

To configure Open Shortest Path Firstly (OSPF) routing switch interconnecting to nonbroadcast networks, use the neighbor command. To remove a configuration, use the no form of this command.

neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*]

no neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [*cost number*]

Parameter

parameter	description
ip-address	Interface IP address of the neighbor.
priority number	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The

	default is 0. This keyword does not apply to point-to-multipoint interfaces.
poll-interval seconds	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.
cost number	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the number argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

Default value

no default value

Command mode

OSPF routing configuration

Usage guidelines

In X.25 and Frame Relay networks you can configure OSPF to run as a broadcast network. Detailed information is as follow:

In X.25 and frame relay map

One nonbroadcast network neighbor must be configured in the routing switch. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive, it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called Poll Interval.

When the routing switch first starts up, it sends only hello packets to those routing switches with nonzero priority, that is, routing switches that are eligible to become designated routeing switch (DRs) and backup designated routing switches (BDRs). After the DRs and BDRsare selected, DRs and BDRs will then start sending hello packets to all neighbors in order to form adjacencies.

Example

The following example declares a routing switch at address 131.108.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
!
router ospf 100
 neighbor 131.108.3.4 priority 1 poll-interval 180
!
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
!
interface VLAN2
  ip address 10.0.1.1 255.255.255.0
  no ip directed-broadcast
  ip ospf network point-to-multipoint non-broadcast
!
!
router ospf 1
  network 10.0.1.0 255.255.255.0 area 0
  neighbor 10.0.1.3 cost 5
  neighbor 10.0.1.4 cost 10
  neighbor 10.0.1.5 cost 15
!
```

Related commands

ip ospf priority

5.1.46 network area

Syntax

To define several network segments in an area as a network range, use the network area command. To disable the feature, use the no form of this command.

network *network mask* **area** *area_id*

no network *network mask* **area** *area_id*

Parameter

parameter	description
network	Network Ip address, in dotted decimal format.
mask	Mask, in dotted decimal format.
area_id	Id of area.

Default value

This command is disabled by default.

Command mode

OSPF Routing configuration mode

Usage guidelines

Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the network command list and ignore the subsequent overlapping portions. Importing network range and specifying the range can reduce the switch state of routing information among areas

Example

The following example defines network range 10.0.0.0 255.0.0.0 and adds to area 2:

Switch_config_ospf_2#network 10.0.0.0 255.0.0.0 area 2

5.1.47 redistribute

Syntax

To configure OSPF to redistribute routes of other routing protocols, use the redistribute command. Use the no form of this command to restore the default.

redistribute *protocol process-id* [**metric-type** [*1* | *2*] | **metric** *cost* | **tag** *tag* | **route-map** *WORD*]

no redistribute *protocol process-id* [**metric | tag | route-map**]

Parameter

parameter	Description
protocol	Redistributes former protocols that learned, it should be one of the following: beigrp, bgp, connect, isis, ospf, rip, static.
process-id	(Optional) Autonomous system number. There is no parameter for connect, static.
metric-type [*1* | *2*]	(Optional) Metric value type. The value ranges from 1 to 2. The default value is 2.
metric *cost*	(Optional) The routing cost value, ranges from 0 to 16777214, and the default value is 100.
tag *tag*	(Optional) The routing tag in the external LSA, in the range of 0 to 4294967295. The default value is 0.
route-map *WORD*	(Optional) Configure the route conforming to the specified routing policy.

Default value

Enabled

Command mode

OSPF Routing configuration mode

Usage guidelines

External route refers to the route to the outside of the autonomous system. This command does not redistribute the default route.

Example

The following example redistributes static route, metric value is Type-1, a route tag is 1000, and a metric value is 10:

Switch_config_ospf_2#redistribute static metric-type 1 tag 1000 metric 10

5.1.48 restart ospf

Syntax

To restart the OSPF process, use the restart ospf command. If no process-id is specified, all OSPF processes are restarted.

restart ospf [*process-id*] [**graceful**]

Parameter

parameter	description
process-id	The number of OSPF process. Range is from 1 to 65535.
graceful	(Optional) Restart OSPF process gracefully without changing Router ID.

Default value

None

Command mode

EXEC

Usage guidelines

Use **restart ospf [process-id]** command to restart the OSPF process, you can get the following results:

(1) You can immediately clear all data structures of the OSPF process.

(2) This command will reselect the Router ID.

(3) The OSPF configuration before restarting will not be lost.

If you restart gracefully, you can achieve uninterrupted forwarding, and the Router ID before and after the restart remains unchanged.

Example

Restart all OSPF processes gracefully:

restart ospf graceful

5.1.49 router-id

Syntax

To designate router-id in OSPF in progesss, run the following command. To return to the default setting, use the no form of this command.

router-id *ip-address*

no router-id

Parameter

Parameter	Description
ip-address	Router ID of OSPF progress. Point spread decimalism

Default value

OSPF progress selects router-id on its own.

Command mode

OSPF Routing configuration mode

Usage guidelines

After configuring the new router-id, the OSPF progress will be restarted. The configured router-id is exclusive to the whole OSPF autonomous domain.

Example

The following example shows how to configure one OSPF progress and the designated router-id is 1.1.1.1:

```
!
router ospf 109
 router-id 1.1.1.1
!
```

Related command

router ospf

5.1.50 router ospf

Syntax

To configure an Open Shortest Path Firstly (OSPF) routing process, use the router ospf command. To terminate an OSPF routing process, use the no form of this command.

router ospf *process-id* [**vrf** *WORD*]

no router ospf *process-id* [**vrf** *WORD*]

Parameter

parameter	description
process-id	ospf process ID. The value ranges from 1 to 65535.
vrf *WORD*	(Optional) Configure the name of the VPN instance bound to the OSPF process.

Default value

No OSPF routing process is defined.

Command mode

Global configuration mode

Usage guidelines

You can specify multiple OSPF routing processes in each router.

On a router, you can run multiple ospf processes by specifying different process numbers. In this case, you can use the **router-id** command to specify different Router IDs for different processes.

If OSPF is used as a VPN internal routing protocol, you need to bind the OSPF process to the VPN instance.

Example

The following example configures an OSPF routing process and assign a process number of 109:

```
router ospf 109
```

Related commands

network area

5.1.51 show ip ospf

Syntax

To display general information about Open Shortest Path Firstly (OSPF), use the show ip ospf command.

show ip ospf [*process-id*]

Parameter

parameter	description
process-id	(Optional) Process ID.

Default value

none

Command mode

EXEC

Usage guidelines

Troubleshoot OSPF problems according to the output of this command. To display only the global configuration information of the corresponding OSPF process if configured with the process-id parameter.

Example

The following display the configuration information of OSPF process :

Switch#show ip ospf

OSPF process: 1, Router ID is 192.168.99.81

Distance: intra-area 110 inter-area 130 external 150

Source Distance Access-list

240.240.1.1/24 1 what

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Number of areas is 3

AREA: 1

Number of interface in this area is 1(UP: 1)

Area authentication type: None

AREA: 36.0.0.1

This is a stub area.

Number of interface in this area is 0(UP: 0)

Area authentication type: None

AREA: 192.168.20.0

Number of interface in this area is 0(UP: 0)

Area authentication type: None

Net Range list:

10.0.0.0/255.0.0.0 Not-Advertise

140.140.0.0/255.255.0.0 Advertise

filter list on receiving UPDATE is Gateway: weewe

filter list on sending UPDATE is Prefix: trtwd

Summary-address list:

150.150.0.0/16 advertise

Switch#

Description of the displaying fields

field	description
OSPF process: 1	OSPF process ID
Router ID is 192.168.99.81	Routing switch ID
Distance: intra-area 110 inter-area 130 external 150	The default administrative distance that the current routing switch adopts
Source Distance Access-list	Administrative distance based on concrete routing configuration
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs	Value of two timer related to OSPF
Number of areas is 3	The number of the field that currently configured and the parameter configured in each field
filter list on receiving...	The configured filter list on receiving routes

filter list on sending	The configured filter list on sending routes
Summary-address list	The configured routing summary address

5.1.52 show ip ospf border-routers

Syntax

To display the internal Open Shortest Path Firstly (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the show ip ospf border-routers command.

show ip ospf border-routers

Parameter

none

Default value

none

Command mode

EXEC

Example

Switch #
Switch #show ip ospf border-routers
OSPF process: 1
Codes: i - Intra-area route, I - Inter-area route
Destination Adv-Rtr Cost Type Area
i 192.168.20.77 192.168.20.77 11 ABR 0
Switch #

Field description:

field	description
Destination	Routing switch ID of the destination.
Adv-Rtr	Next hop toward the destination.
Cost	Cost of using this route.
Type	The routing switch type of the destination; it is either an ABR or ASBR or both.

Area	The area ID of the area from which this route is learned.

5.1.53 show ip ospf database

Syntax

To display lists of information related to the Open Shortest Path Firstly (OSPF) database, use the show ip ospf database command.

show ip ospf database

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

Display lists of information related to the Open Shortest Path Firstly (OSPF) database in accordance with debugging information of the command, and it is helpful for users in troubleshooting

Example

Switch #show ip ospf database

OSPF process: 1

(Router ID 192.168.99.81)

AREA: 0

Router Link States

Link ID ADV Router Age Seq # Checksum Link count

192.168.20.77 192.168.20.77 77 0x8000008a 0x90ed 1

192.168.99.81 192.168.99.81 66 0x80000003 0xd978 1

Net Link States

Link ID ADV Router Age Seq # Checksum

192.168.20.77 192.168.20.77 80 0x80000001 0x9625

Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.99.0 192.168.99.81 87 0x80000003 0xd78c
AREA: 1
Router Link States
Link ID ADV Router Age Seq # Checksum Link count
192.168.99.81 192.168.99.81 70 0x80000002 0x0817 1
Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.20.0 192.168.99.81 66 0x80000006 0xd1c1
Switch #

Field description:

field	Description
AREA: 1	OSPF area.
Router Link States/Net Link States/Summary Net Link States	LSA type
Link ID	LSA ID.
ADV Router	Advertising routing switch's ID.
Age	Link state age.
Seq #	Link state sequence number
Checksum	Fletcher checksum of the complete contents of the link state advertisement.

5.1.54 show ip ospf interface

Syntax

To display Open Shortest Path Firstly (OSPF)-related interface information, use the show ip ospf interface command.

show ip ospf interface

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display configuration and operation situation of OSPF on an interface according to the debugging information of this command. Users can confirm whether the configuration is right or not and it is helpful in troubeshooting

Example

```
Switch #show ip ospf interface
VLAN1 is up, line protocol is up
  Internet Address: 10.0.1.1/24
  Interface index: 34, 0x4057ea8
  Nettype: Point-to-MultiPoint with Non-Broadcast
  OSPF process is 1, AREA: 0, Router ID: 192.168.30.81
      Cost: 1, Priority 1, Transmit Delay is 1 sec
  Hello interval is 30, Dead timer is 120, Retransmit is 5
  OSPF INTF State is IPOINT_TO_MPOINT
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 1.0.4.1
  Null authentication enabled
Switch #
```

Displaying field description:

field	description
Internet Address:	Interface IP address
Nettype	Net type of OSPF interface
OSPF process is	OSPF process number
AREA	OSPF area.
Router ID	Routing switch ID
Cost	Cost of routing switch OSPF interface
Transmit Delay is	Transmit delay
Priority	Priority of routing switch interface
Hello interval	Number of seconds until next hello packet is sent out this interface.
Dead timer	Dead timer
Retransmit	Retransmit interval
OSPF INTF State is	OSPF nterface state

5.1.55 show ip ospf neighbor

Syntax

To display Open Shortest Path Firstly (OSPF)-neighbor information, use the show ip ospf neighbor command.

show ip ospf neighbor [detail]

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

To display neighbor situation of OSPF from the output of this command to help user troubleshoot OSPF.

Example

Switch#show ip ospf neighbor

AREA: 0

Neighbor ID Pri State DeadTime Neighbor Addr Interface

1.0.4.1 0 FULL/- 100 10.0.1.3 VLAN1

Displaying field description:

field	description
OSPF process	OSPF process number
AREA	OSPF area
Neighbor	Neighbor routing switch ID.
Pri	Routing switch priority of the neighbor, neighbor state.
State	OSPF state.
DeadTime	Expected time before software will declare the neighbor dead.
Neighbor Addr	Neighbor ip address

Interface	Interface to which connects the neighbor

5.1.56 show ip ospf virtual-link

Syntax

To display information of Open Shortest Path Firstly (OSPF) virtual links, use the show ip ospf virtual-links command.

show ip ospf virtual-link

Parameter

none

Default value

none

Command mode

EXEC

Usage guidelines

The information displayed by the show ip ospf virtual-links command is useful in debugging OSPF routing operations. To display the detailed information of adjacency relation of the OSPF neighbour, use the show show ip ospf neighbour command

Example

Switch#show ip ospf vir

Virtual Link Neighbor ID 200.200.200.2 (UP)

Run as Demand-Circuit

TransArea: 1, Cost is 185

Hello interval is 10, Dead timer is 40 Retransmit is 5

INTF Adjacency state is IPOINT_TO_POINT

Description of the displaying fields:

field	description
neibhbor ID	The configured neighbor ID of the remote side
neighbour state	Adjacency relation of the OSPF neighbor
Demand-Circuit	Indicates working under DC mode

TransArea	The transit area through which the virtual link is formed.
cost	The cost of reaching the OSPF neighbor through the virtual link.
Hello Interval	The current Hello interval
DeadTime	Expected time before software will declare the neighbor dead.
Retrans	Retransmit interval
INTF Adjacency State	The state of virtual link.

Related commands

area vritual-link

show ip ospf neighbor

5.1.57 stub-router

Syntax

To set stub route, rrun the following command. To return to the default setting, use the no form of this command.

stub-router

no stub-router

Parameter

None

Default value

Disabled

Command mode

OSPF Routing configuration mode

Usage guidelines

After the router is configured as Stub router, the router will not forward packets whose destination segment is not in the router. At the moment, in Router-LSA published by the router, the value of the link whose type is 1 (point to point link), 1(connecting to the transmission network) and 4 (virtual link) will be set as 65535, while the value of the link 3 (connecting to Stub network) will not be changed. Thus, when other routers are working, if there is a smaller router with less cost in the destination address, the data will not be forwarded by this Stub router.

Example

The following example shows how to configure Stub router as the local router:

```
router ospf 109
   stub-router
```

5.1.58 summary-address

Syntax

To create aggregate addresses for Open Shortest Path Firstly (OSPF), use the summary-address command. To restore the default, use the no form of this command.

summary-address *address mask* [**not-advertise | tag** *value*]

no summary-address *address mask*

Parameter

parameter	description
address	Summary address designated for a range of addresses.
Mask	IP subnet mask used for the summary route.
not-advertise	(Optional) Suppress match routes that creat LSA
tag	(Optional) Set route tag
value	Route tag value, the range is from 0 to 4294967295, the default is 0.

Default value

none

Command mode

OSPF Routing configuration mode

Usage guidelines

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Routing switch (ASBRs) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the area range command for route summarization.

Example

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

summary-address 10.1.0.0 255.255.0.0

Related commands

area range

ip ospf password

ip ospf message-digest-key

5.1.59 timers delay-timer

Syntax

To specify the delay interval between OSPF receiving a topology structure variety and initializing a minimum route priority computation, use the **timers delay-timer** command. Use the no form of this command to resotre default value.

timers delay-timer *spf-delay*

no timers delay-timer

Parameter

parameter	description
spf-delay	Delay between topology variety and computation commencement in seconds, from 0 to 65535. Default value is 5 seconds. If the value is 0, that indicates there is no delay, namely, once there is a variety, the commencement of computation immediately starts.

Default value

spf-delay: 5 seconds

Command mode

OSPF Routing configuration mode

Usage guidelines

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

Example

timers delay-timer 10

5.1.60 timers hold-timer

Syntax

To configure the interval between two continuous SPF computation, use the timers hold command. Use the no form of this command to restore the default value.

timers hold-timer *spf-holdtime*

no timers hold-timer

Parameter

parameter	description
spf-holdtime	The minimum value between two continuous computation, in the range from 0 to 65535. The default value is 10 seconds; 0 means that there is no time difference between two consecutive calculations.

Default value

spf-holdtime: 10 seconds

Command mode

OSPF Routing configuration mode

Usage guidelines

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

Example

timers hold-timer 20

5.1.61 timers age-timer

Syntax

To set time interval of OSPF checking LSA database aging, run the following command. To return to the default setting, use the no form of this command.

timers age-timer *agetime*

no timers age-timer

Parameter

Parameter	Description
agetime	Check lsa database every agetime

Default value

agetime: 60s

Command mode

OSPF Routing configuration mode

Usage guidelines

The smaller the time, the faster the database responds, but with more processer time.

Example

timers age-timer 50

Chapter 6 BGP Configuration Commands

6.1 BGP Configuration Commands include:

- address-family ipv4
- address-family ipv6
- address-family vpnv4
- aggregate-address
- bgp always-compare-med
- bgp asnotation dot
- bgp bestpath med
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp dampening
- bgp default local-preference
- bgp default route-target filter
- bgp deterministic-med
- bgp fast-external-fallover
- bgp graceful-restart
- bgp update-delay
- bgp maxas-limit
- bgp router-id
- bgp update-delay
- clear ip bgp
- debug ip bgp
- distance

- filter
- maximum-paths
- neighbor activate
- neighbor advertisement-interval
- neighbor allowas-in
- neighbor capability orf prefix-list
- neighbor default-originate
- neighbor description
- neighbor distribute-list
- neighbor ebgp-multihop
- neighbor fall-over
- neighbor filter-list
- neighbor local-as
- neighbor maximum-prefix
- neighbor next-hop-self
- neighbor password
- neighbor peer-group
- neighbor prefix-list
- neighbor remote-as
- neighbor remove-private-AS
- neighbor route-map
- neighbor route-reflector-client
- neighbor route-refresh
- neighbor send-community
- neighbor send-label
- neighbor shutdown
- neighbor soft-reconfiguration
- neighbor timers
- neighbor ttl-security-hop

- neighbor update-source
- neighbor weight
- network (BGP)
- redistribute (BGP)
- router bgp
- show ip bgp
- show ip bgp community
- show ip bgp neighbors
- show ip bgp paths
- show ip bgp prefix-list
- show ip bgp regexp
- show ip bgp summary
- synchronization
- table-map
- timers

6.1.1 address-family ipv4

Syntax

To eneter bgp ipv4 address family mode, run the following command. To return to the default setting, use the no form of this command.

address-family ipv4 {mdt | multicast | unicast | vrf} [name]

Parameter

Parameter	Description
mdt	Enters ipv4 mdt configuration mode. It is used for mvpn.
multicast	Enters ipv4 multicast configuration mode. It is used for multicast rpf query.
unicast	Enters ipv4 unicast configuration mode. It is used for ipv4 unicast.
name	Configuration parameters of address-family ipv4 vrf, which means enter vpn configuration mode.

Default value

None

Command mode

BGP configuration mode

Usage guidelines

Expand bgp configuration mode.

Example

The following example shows how to activate neighbor 1.1.1.1 ipv4 mdt route inform.

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1

 address-family ipv4 mdt
 neighbor 1.1.1.1 activate
 exit-address-family
```

Related command

exit-address-family

6.1.2 address-family ipv6

Syntax

To enter bgp ipv6 address family configuration mode, run the following command.

address-family ipv6 {multicast | unicast}

Parameter

Parameter	Description
multicast	Enters the configuration mode of ipv6 multicast.
unicast	Enters the configuration mode of ipv6 unicast.

Default value

None

Command mode

BGP configuration mode

Usage guidelines

Expand bgp configuration mode

Example

The following example shows how to activate neighbor 1.1.1.1 ipv6 routing inform:

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1

 address-family ipv6
 neighbor 1.1.1.1 activate
 exit-address-family
```

Related command

exit-address-family

6.1.3 address-family vpnv4

Syntax

To enter bgp vpnv4 address family configuration mode, run the following command.

address-family vpnv4

Parameter

None

Default value

None

Command mode

BGP configuration mode

Usage guidelines

Expand bgp configuration mode: used for l3vpn configuration environment. The configuration mode is often used in condition of PE-PE interconnection.

Example

The following example shows how to activate neighbor 1.1.1.1 vpnv4 routing inform.

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1

 address-family vpnv4
 neighbor 1.1.1.1 activate
 exit-address-family
```

Related command

exit-address-family

6.1.4 aggregate-address

Syntax

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the aggregate-address command in address family or routing switch configuration mode. To disable this function, use the no form of this command.

aggregate-address A.B.C.D/n [as-set] [**summary-only**] [**attribute-map** *map-name*]

no aggregate-address A.B.C.D/n

Parameter

parameter	description
A.B.C.D/n	Aggregate network
as-set	Including AS set path attribute (AS-SET) of aggregated routes.
summary-only	Filters all more-specific routes from updates.
attribute-map	Name of the route map used to set the attribute of the aggregate route.
map-name	Name of the route map

Default value

none

Command mode

BGP configuration mode

Usage guidelines

You can implement aggregate routing in BGP in three methods: first,dynamic implement routing by forwarding redistribute; second, static implement routing by network command; third, static implement routing by aggregate. The routing created in this way are local routing, which can be announced to other equivalent, but not implement local IP address table.

The generation of aggregation routes is to reduce the number of routes in the routing table and increase the efficiency of route indexes and the stability of routes. BGP aggregation routes are performed in the BGP routing table, and aggregation routes are considered as locally generated routes and will not be added to the routes table. But they can be seen in the BGP routing table. The aggregate-address command with the same prefix will override the original configuration.

Aggregation routes usually aggregate existing routes according to certain rules. The existence of this route depends on the status of the its source route. BGP aggregation routes rely on the routes with the same prefix and more precise routes in the BGP routing table. When there is at least one route with the same prefix or a more precise route in the BGP routing table, the aggregation route can be valid. When the aggregation route is valid, it can be displayed by **show ip bgp** command, with a *> mark. The aggregation route can suppress the source route, then it is marked with s.

Without the as-set option, the as-path attribute formation of the aggregation route follows the following rules:

All entries that appear in as-sequence should appear in the summarized as-path;

All entries that appear in as-set must appear in at least one type of summarized as-path;

The longest identical entry in as-sequence is used as the summarized as-sequence;

The remaining entries are as-set.

With the as-set option, the as-path attribute of all existing routes appears in the as-path of the aggregate route as as-set.

Using the **summary-only** option not only creates an aggregation route (for example, 193.*.*.*), but also suppresses more specific routes.

Use the **attribute-map** option to modify the attributes of the route when generating an aggregate route.

The maximum number of aggregate commands that can be configured is determined by the switch resources, such as the configured RAM.

Example

In the following example, an aggregate BGP address is created :

router bgp 5

aggregate-address 193.0.0.0/8

Related commands

route-map

6.1.5 bgp always-compare-med

Syntax

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the bgp always-compare-med command. To disallow the comparison, use the no form of this command.

bgp always-compare-med

no bgp always-compare-med

Parameter

none

Default value

Not compare the MED for paths from neighbors in different autonomous systems.

Command mode

BGP configuration mode

Usage guidelines

Generally speaking, when BGP selects routes, only two from the same autonomous system can compare MED. Using **bgp always-comapre-med** command can make BGP always compare MED, regardless of whether the route comes from the same autonomous system. This can change the route selection process.

Example

The following example enables the function

```
router bgp 5
bgp always-compare-med
```

Related commands

bgp bestpath med

bgp deterministic-med

6.1.6 bgp asnotation dot

Syntax

To enable asdot mode, run the following command.

bgp asnotation dot

no bgp asnotation dot

Parameter

None

Default value

asplain mode

Command mode

BGP configuration mode

Usage guidelines

The command is used to configure the display form of as. Only when as is greater than 65535 can it is displayed in the form of asdot. The command takes effect needs to activate **clear ip bgp ***.

Example

The following example shows how to enable the function:

```
router bgp 100
bgp asnotation dot
```

Related command

route bgp

show ip bgp

6.1.7 bgp bestpath med

Syntax

To modify the process way of Border Gateway Protocol (BGP) on Multi Exit Discriminator (MED) attribute, use the **bgp bestpath med** command. To disable the feature, use the no form of this command.

bgp bestpath med {**confed | missing-as-worst**}

no bgp bestpath med {**confed | missing-as-worst**}

Parameter

parameter	description
confed	Autonous system confederation MED comparison attrubute
missing-as-worst	(Optional) Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable.

Default value

none

Command mode

BGP configuration mode

Usage guidelines

If the MED attribute of BGP route is not configured, the value of MED is always considered to be 0, that is the least value, which has the most priority. When configured with the missing-as-worst option, if the MED attribute of BGP route is not configured, the value of MED is always considered to be the most maximum value, which has the least priority.

By default, the same routes advertised by different BGP switches within the same autonomous system are compared to MED, while within the same autonomous system alliance, the same routes advertised by different autonomous systems are not compared to MED. After t all the same routes advert he confed option is configured, this rule is modified to make ised within the same autonomous system alliance compare MED.

Example

By default, the MED comparison between (100)and (200) doesn't occur for they are not the routes from the same sub-autonomous system. But the MED comparison occurs when configured with the bgp bestpath med confed command, for they come from the sub-autonomous system 100 and 200 respecitively in the autonomous system alliance.

Related commands

bgp always-compare-med

bgp deterministic-med

6.1.8 bgp client-to-client reflection

Syntax

To enable or restore route reflection from a BGP route reflector to clients, use the bgp client-to-client reflection command. To disable client-to-client route reflection, use the no form of this command.

bgp client-to-client reflection

no bgp client-to-client reflection

Parameter

none

Default value

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command mode

BGP configuration mode

Usage guidelines

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the no bgp client-to-client reflection command to disable client-to-client reflection.

Example

In the following example, the local routing switch is a route reflector, and the three neighbors are fully meshed, turn off client-to-client reflection

router bgp 5

neighbor 192..168.20.190 router-reflector-client

neighbor 192..168.20.191 router-reflector-client

neighbor 192..168.20.192 router-reflector-client

no bgp client-to-client reflection Related commands

neighbor route-reflector-client

bgp cluster-id

6.1.9 bgp cluster-id

Syntax

bgp cluster-id *cluster-id*

no bgp cluster-id [*cluster-id*]

Parameter

parameter	description
cluster-id	Cluster ID of this router acting as a route reflector, which can be a IP address or a number; maximum of 4 bytes.

Default value

The local routing switch ID of the route reflector is used as the cluster ID when no ID is specified or when the no form of this command is entered.

Command mode

BGP configuration mode

Usage guidelines

Together, one or more route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the routing switch ID of the route reflector. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. This allows all route reflectors in the cluster must be configured with a 4-byte cluster ID to recognize updates from peers in the same cluster.

When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors.

Example

In the following example, the local routing switch is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster. Neighbor 198.92.70.24 is a route reflection client:

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
bgp cluster-id 50000
```

Related commands

neighbor route-reflector-client

show ip bgp summary

6.1.10 bgp confederation identifier

Syntax

To specify a BGP confederation identifier, use the bgp confederation identifier command. To remove the confederation identifier, use the no form of this command.

bgp confederation identifier autonomous-system

no bgp confederation identifier autonomous-system

Parameter

parameter	description
autonomous-system	Autonomous system number to be configured to internally include multiple autonomous systems.

Default value

none

Command mode

BGP configuration mode

Usage guidelines

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. In the Autonomous System Alliance, an AS that can be divided into several sub-ASs. Within each sub-AS, all IBGP rules apply, such as all IBGP neighbors must form a full mesh structure. Each sub-AS has a different AS number, so they EBGP must be run between sub-ASs. Although EBGP is used between sub-ASs, the routing performance within the confederation is similar to the IBGP routing within a single AS. That is, when crossing the boundaries of sub-ASs, Nexthop, MED, Localpreference information is preserved. To the others, the alliance looks like a single AS.

An autonomous system alliance identifier is an autonomous system. All BGP switches in the same autonomous system alliance must be configured with the same autonomous system alliance identifier.

Configuring the autonomous system alliance identifier often requires re-establishing BGP connections.

Example

In the following example, the routing domain is divided into autonomous systems AS4001, 4002, 4003, 4004, 4005, 4006 and 4007 and identified by the confederation identifier 5. The local AS is 4001. Neighbor 1.2.3.4 is a peer inside of the routing domain confederation. Neighbor 3.4.5.6 is a peer outside of the routing domain confederation. For the neighbor 3.4.5.6, your AS is 5:.

```
router bgp 4001
bgp confederation identifier 5
bgp confederation peers 4002 4003 4004 4005 4006 4007
neighbor 1.2.3.4 remote-as 4002
neighbor 3.4.5.6 remote-as 510
```

Related commands

bgp confederation peers

show ip bgp summary

6.1.11 bgp confederation peers

Syntax

To configure subautonomous systems to belong to a single confederation, use the bgp confederation peers command in router configuration mode. To remove an autonomous system from the confederation, use the no form of this command.

bgp confederation peers autonomous-system [**autonomous-system**]

no bgp confederation peers [**autonomous-system**]

Parameter

parameter	description
autonomous-system	Autonomous system number

Default value

none

Command mode

BGP configuration mode

Usage guidelines

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. In the Autonomous System Alliance, an AS that can be divided into several sub-ASs. Within each sub-AS, all IBGP rules apply, such as all IBGP neighbors must form a full mesh structure. Each sub-AS has a different AS number, so they EBGP must be run between sub-ASs. Although EBGP is used between sub-ASs, the routing performance within the confederation is similar to the IBGP routing within a single AS. That is, when crossing the boundaries of sub-ASs, Nexthop, MED, Localpreference information is preserved. To the others, the alliance looks like a single AS.

The autonomous system specified by this command is internal to the same autonomous system alliance and is a sub-autonomous system. Each sub-autonomous system is fully connected within itself.

Generally, use the **bgp confederation identifier** command to specify which autonomous system alliance the local AS belongs to.

Configuring this command often requires re-establishing BGP connections.

Example

In the following example, autonomous systems 1091, 1092 and 1093 are configured to belong to a single confederation under the identifier 1090:

```
router bgp 1090
bgp confederation identifier 23
bgp confederation peers 1091 1092 1093
```

Related commands

bgp confederation identifier

show ip bgp summary

6.1.12 bgp dampening

Syntax

To enable BGP route dampening or change BGP route dampening parameters, use the **bgp dampening** command. To disable BGP dampening, use the no form of this command.

bgp dampening [*half-time resuse-value suppress-value hold-time*]

no bgp dampening

Parameter

parameter	description
half-time	Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period.
reuse-value	Reuse values based on accumulated penalties.
suppress-value	A route is suppressed when its penalty exceeds this limit.
hold-time	Maximum time (in minutes) a route can be suppressed.

Default value

half-time: 15 minutes

reuse-value: 750

suppress-value: 2000

hold-time: 60 minutes

Command mode

BGP configuration mode

Usage guidelines

Route fluctuation control has different effects on routes in different states, mainly affecting whether the route is advertised to neighbors and whether it can be aggregated, and whether it is added to the main routing table. According to the fluctuation process of a route, its changes are described as follows:

A stable route is punished due to fluctuations. When its penalty value is less than the minimum penalty value of the suppressed route, it continues to advertise to neighbors and can be aggregated; when the penalty value of the route exceeds the Suppress value, it stops advertising to neighbors and stop being aggregated; when the route is stable, its penalty value can be reduced with time. It is always in a suppressed state until its penalty value reaches the maximum penalty value of the reused route (Reuse), and it cannot advertise to neighbors and be aggregated; When the penalty value drops below Reuse, the route becomes effective and can advertise to neighbors and be aggregated.

Example

In the following example, the bgp dampening command can be used to enable BGP route dampening function and use default parameter configuration. Use the following commands to configure different dampening parameters for different rouing configurations:

```
Router bgp 100
bgp dampening
```

Related commands

None

6.1.13 bgp default local-preference

Syntax

To configure default parameter of BGP process, use the bgp default command. Use the no form of this command to restore the default value.

bgp default local-preference <*0-4294967295*>

no bgp default local-preference

Parameter

parameter	description
local-preference	Configures default parameter of the local preference.
<0-4294967295>	Default value of the local preference

Default value

100

Command mode

BGP configuration mode

Usage guidelines

The route received from IBGP will be set as the local preference by BGP. The default value is 100, which can be modified via this command.

Example

The following example configures 200 as the local preference for the route from IBGP neighbor:

```
router bgp 100
bgp default local-preference 200
```

Related commands

None

6.1.14 bgp default route-target filter

Syntax

To set BGP VPN route filter function, run the following command. To return to the default setting, use the no form of this command.

bgp default route-target filter

no bgp default route-target filter

Parameter

None

Default value

Enabled

Command mode

BGP configuration mode

Usage guidelines

The command is enabled by default. It is used to control VPN multi-communication. To disable the filter function, run the command “no bgp default route-target filter”, which means all VPN routes are received, generally applied to the solution of cross-domain VPN option-B.

Example

The following example shows how to enable all VPN routes passing.

```
router bgp 100
no bgp default route-target filter
```

Related command

None

6.1.15 bgp deterministic-med

Syntax

To modify BGP's handling of MED attributes, use the following command. To restore the default values, use no form of the command.

bgp deterministic-med

no bgp deterministic-med

Parameter

none

Default value

none

Command mode

BGP configuration mode

Usage guidelines

By default, comparison of the Multi Exit Discriminator (MED) for routes from different neighbors in the same autonomous systems is enabled. The **bgp bestpath med confed** command is used to enable the comparison of the Multi Exit Discriminator

(MED) for routes from different neighbors in the same autonomous systems alliance. This command is to make BGP compare MED to routes from different neighbors with the same autonomous system and the same sub-autonomous system.

Example

none

Related commands

bgp bestpath med

bgp always-compare-med

6.1.16 bgp fast-external-fallover

Syntax

To enable fast clear neighbor function, run the following command. To return to the default setting, use the no form of this command.

bgp fast-external-fallover

no bgp fast-external-fallover

Parameter

None

Default value

Enabled

Command mode

BGP configuration mode

Usage guidelines

The function is enabled by default. If the interface status becomes **Down**, it will immediately clear the BGP dialogue of the direct external neighbor on the interface.

Example

None

Related command

router bgp

clear ip bgp

6.1.17 bgp graceful-restart

Syntax

To configure bgp graceful restart, run the following command.

bgp graceful-restart [**restart-time** value] **|** [**stalepath-time** value]

no bgp graceful-restart [restart-time] **|** [stalepath-time]

Parameter

Parameter	Description
restart-time	To configure the max waiting time of protocol restarting neighbor up. The default value is 120s.
stalepath-time	To configure the max stalepath time of restarting the neighbor and aging the route. The default value is 360s.

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

bgp graceful-restart restart-time

The command is used to configure Restart Time of BGP GR, which is used by Receiving Speaker

bgp graceful-restart stalepath-time

The configuration time should be the time of keeping aging route.

Example

None

Related command

bgp update-delay

clear ip bgp

6.1.18 bgp maxas-limit

Syntax

To configure the max amount limit of as which bgp route passes, run the following command.

bgp maxas-limit <value>

no bgp maxas-limit

Parameter

Parameter	Description
value	The value ranges from 1 to 500.

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to limit the amount of **as** which is part of **aspath** of routes received by the neighbor. The value will de dropped if the amount of **as** is greater than the configured value.

Example

None

Related command

clear ip bgp

6.1.19 bgp router-id

Syntax

To configure bgp router identifier, run the following command.

bgp router-id *<A.B.C.D>*

no bgp router-id *<A.B.C.D>*

Parameter

Parameter	Description
A.B.C.D	To be configured ID.

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to configure a new router ID. Peer in the state of Established will automatically resume to BGP.

Example

None

Related command

clear ip bgp

show ip bgp

6.1.20 bgp update-delay

Syntax

To configure bgp route update delay, run the following command. To return to the default setting, use the no form of this command.

bgp update-delay <value>

no bgp update-delay

Parameter

Parameter	Description
value	Time of the route update delay. The value ranges from 1 to 3600s.

Default value

360s

Command mode

BGP configuration mode

Usage guidelines

The command takes effect only when BGP supports GR. After BGP restart, BGP will not send the firstly update packets to local RIB until the timer is overtime. The BGP process re-selects the optimal route and then advertises it. That is to say, after BGP restarts, BGP will wait until this timer expires before sending the first update message.

Another condition is that BGP updates without waiting for overtime of the timer. Refer to the command “**bgp graceful restart**” for more information.

Example

None

Related command

bgp graceful-restart

clear ip bgp

6.1.21 bgp redistribute-internal

Syntax

To configure IBGP redistribution into an interior gateway protocol (IGP), such as RIP or OSPF, use the **bgp redistribute-internal** command. To return the router to default behavior and stop iBGP redistribution into IGPs, use the no form of this command.

bgp redistribute-internal

no bgp redistribute-internal

Parameter

none

Default value

IBGP routes are not redistributed into IGP.

Command mode

BGP configuration mode

Usage guidelines

When configuring this command, you must pay attention to the configuration between the switches, otherwise it is easy to cause routing loops. After configuring this command, use the command **clear ip bgp *** to reset BGP.

Example

In the following example, BGP to OSPF3 route redistribution is enabled:

```
router ospf 3
 redistribute bgp 2
!
router bgp 2
 bgp redistribute-internal
!
```

Related commands

None

6.1.22 clear ip bgp

Syntax

To reset Border Gateway Protocol (BGP) connections using soft reconfiguration, use the clear ip bgp command.

clear ip bgp {* | *ip-address* | ipv6-address | as-number |dampening | **peer-group** *name* **| aggregates | networks | redistribute}** [**soft** [**in** [prefix-filter]]**| out]]**

Parameter

parameter	description
*	Specifies that all current BGP sessions will be reset.
ip-address	Specifies that only the identified BGP neighbor will be reset.
ipv6-address	Reset the specified IPv6 address neighbor.
as-number	Specifies that sessions with BGP peers in the specified autonomous system will be reset.
dampening	Clear routing information suppressed by fluctuations.
peer-group name	Specifies that the identified BGP peer group will be reset.
aggregates	Specifies that all aggregate routes will be reset.
networks	Specifies that all static network routes will be reset.
redistribute	Specifies that all redistributed routes will be reset.
soft	Initiates a soft reset.
in | out	Initiates inbound or outbound reconfiguration.
prefix-filter	Soft reconfiguration of ORF inbound routin.

Command mode

EXEC

Usage guidelines

Some BGP policy configurations will not take effect immediately, because the route will only be sent once in a BGP session, so you need to reset the BGP session to send the routing information again.

If the BGP soft reconfiguration is specified by command with the **soft** keyword, the session will not be reset, and the switch sends all the routing update information again. To generate new inbound update information without resetting the BGP session, local BGP session participants should use **neighbor soft-reconfiguration** command to stores all updates received without modification, regardless of whether it is received by the inbound policy. Because this process has a large amount of storage, it should be avoided as much as possible. Outbound BGP soft configuration does not require any additional memory overhead. You can trigger an outbound reconfiguration at the other end of the BGP session to make the new inbound policy take effect.

When using **aggregates, networks, and redistribute,** the **soft** option cannot be used. They will clear the specified type of route and regenerate a new one to make the new configuration take effect.

Example

The following example reset all the current BGP sessions:

```
clear ip bgp *
```

Related commands

neighbor soft-reconfiguration

show ip bgp

6.1.23 debug ip bgp

Syntax

To display information related to processing of the Border Gateway Protocol (BGP), use the **debug ip bgp** command. To disable debugging output, use the no form of this command.

debug ip bgp {all | dampening | event | fsm | keepalive | notify | open | vrf | update }

no debug ip bgp {all | dampening | event | fsm | keepalive | notify | open | vrf | update }

Parameter

parameter	description
all	Displays all BGP debugging functions.
dampening	Displays BGP dampening.
event	Displays BGP events.
fsm	Displays BGP fsms
keepalive	Displays BGP keepalives.
notify	Displays BGP notifies
open	Displays BGP opens
vrf	Enable BGP vrf configuration information tracking.

update	Displays BGP updates.

Default value

All tracking functions are disabled.

Command mode

EXEC

Usage guidelines

It is valid globally when configured with the **debug ip bgp** command to display debugging information. If other VTY are configured with the terminal monitor command, the debugging information will also be displayed. Use the **no terminal monitor** to close this function to disable displaying any debugging information on the VTY.

The command **debug ip bgp all** can enable all BGP debugging function, including dampening, fsm,keepalives,open and update. Use the **no debug ip bgp all** command to disable all BGP debugging functions.

Example

The following example is the process to establish a BGP. The debugging information shows that a switch establishes a connection with BGP neighbor 10.1.1.3. The status changes from Idle to Established, indicating that the connection is established. Various packets information includes receiving Open, sending Open message, sending Keepalive, receiving Keepalive, etc.

The format of the debugging information includes several main parts. The first may be time information, which depends on whether the configuration allows time information to be adde. The information that really belongs to BGP is behind the time information: first indicates the information is about the BGP header information "BGP:", then the specific BGP neighbor address, and then the specific BGP event information.

```
BGP: 10.1.1.3 start connecting to peer
BGP: 10.1.1.3 went from Idle to Connect
BGP: 10.1.1.3 went from Connect to OpenSent
BGP: 10.1.1.3 send OPEN, length 41
BGP: 10.1.1.3 recv OPEN, length 41
BGP: 10.1.1.3 went from OpenSent to OpenConfirm
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 recv KEEPALIVE, length 19
BGP: 10.1.1.3 went from OpenConfirm to Established
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 recv KEEPALIVE, length 19
BGP: 10.1.1.3 recv KEEPALIVE, length 19
```

6.1.24 distance

Syntax

To configure the administrative distance for BGP routes, use the **distance** command. To return to the administrative distance to the default value, use the no form of this command.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Parameter

parameter	description
external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The default value is 20.
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The default value is 200.
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The default value is 200.

Default value

external-distance: 20

internal-distance: 200

local-distance: 200

Command mode

BGP configuration

Usage guidelines

The **distance** command is used to modify the management distance of the route, the priority of the route, and the route selection, to achieve the routing management strategy.

Changing the managemen distance of a route is dangerous unless you know exactly what you are doing. This action may increase the inconsistency of the routing table, which may damage the routing

Example

In the following example, the administrative distance for BGP routes is set:

```
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
distance 20 20 200
```

Related commands

set metric

set tag

6.1.25 filter

Syntax

To filter routes based on an interface in order to realize the administrative strategy. Use the no form of this command to delete the configuration.

filter interface <**in | out**> **{ access-list** *access-list-name* **| gateway** *access-list-name* **| prefix-list** *prefix-list-name* **}**

no filter interface <**in | out**> **{ access-list** *access-list-name* **| gateway** *access-list-name* **| prefix-list** *prefix-list-name*

Parameter

parameter	description
interface	Interface name. Asterisk signifies all interfaces.
in | out	Filter the incoming of outgoing routes
access-list	Specifies the access-list to filter routes
access-list-name	Name of the access list
gateway	Specifies the access list to filter gateway
access-list-name	Name of the access list
prefix-list	Specifies the prefix list to filter routes
prefix-list-name	Name of the prefix list

Default value

none

Command mode

BGP configuration mode

Usage guidelines

The **access-list** option specifies the access list to filter network prefix of routes; the **gateway** option specifies the access list to filter nexthop attribute of routes; the **prefix list** option specifies the prefix list filter network prefix of routes.

The **access list** and the **prefix list** options are mutually exclusive simultaneously. But then can be used with the **gateway** option together.

The asterisk(*) signifies all interfaces. If the filtering rules are configured on the specific interface and all interfaces, the route must meet all the filtering rules.

If a none-existant **prefix list** or **access list** is configured on an interface, then all routes will pass.

Example

The following example configures prefix-list and gateway to filter routes received on all interface:

```
router bgp 109
filter * in prefix-list prefix-guize gateway gateway-guize
```

Related commands

neighbor distribute-list

neighbor filter-list

neighbor route-map

6.1.26 maximum-paths

Syntax

To enable bgp supporting equivalent route, run the **maximum-paths** command. To return to the default setting, use the no form of this command.

maximum-paths [*value*] [**ibgp** value]

no maximum-paths [*value* **|** **ibgp**]

Parameter

Parameter	Description
value	Max amount of the equivalent route supported by BGP

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to modify the amount of bgp supported equivalent routes. Parameters without ibgp is the modified amount of the EBGP equivalent route, which will not affect the choosing result of the optimized routes.

Example

The following example shows how to set the equivalent route which supports 3 ibgp:

```
router bgp 100
maximum-paths ibgp 3
```

Related command

clear ip bgp

show ip bgp

6.1.27 neighbor activate

Syntax

To activate the specified neighbor corresponded address family routing information, run the **neighbor** command. To return to the default setting, use the no form of this command.

neighbor {*ip-address*| *X:X::X:X* | *peer-group-name*} **activate**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **activate**

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	Ipv6 address of the neighbor
peer-group-name	Peer group name

Default value

Activated

Command mode

BGP address protocol stack configuration mode

Usage guidelines

The command is used to activate the support for the specified neighbor corresponded address family routing information.

Example

None

Related command

neighbor remote-as

6.1.28 neighbor advertisement-interval

Syntax

To set the minimum interval of forwarding UPDATE information, run the following command. To return to the default setting, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **advertisement-interval** *value*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **advertisement-interval**

Parameter

Parameter	Description
ip-address	IP address of the neighbor

X:X::X:X	Ipv6 address of the neighbor
peer-group-name	BGP peer group name
Value	<1-600> Unit: s

Default value

ibgp: The default value is 1s.

ebgp: The default value is 30s.

Command mode

BGP configuration mode

Usage guidelines

The command is used to set the minimum interval of forwarding UPDATE information

Example

The following example shows how to set the minimum interval of the neighbor 10.10.10.11 forwarding UPDATE information to 15s.

```
router bgp 1
neighbor 10.10.10.11 remote-as 2
neighbor 10.10.10.11 advertisement-interval 15
```

Related command

neighbor remote-as

6.1.29 neighbor allowas-in

Syntax

To enable BGP receiving route which including **as** from the neighbor learned **aspath**, run the following command. To disallow receiving similar routes, use no form of the command.

neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **allowas-in** [*value*]

no neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **allowas-in**

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
Value	<1-10> Times which enable locak as appeared in the attribute of aspath. The default value is 3.

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

The command is used to enable BGP receiving route which including **as** from the neighbor learned **aspath**

Example

The following example shows how to enable BGP receiving route which including **as** (3 times in maximum) from the neighbor (10.10.10.11) learned **aspath**:

```
router bgp 1
neighbor 10.10.10.11 remote-as 2
neighbor 10.10.10.11 allowas-in
```

Related command

neighbor remote-as

6.1.30 neighbor capability orf prefix-list

Syntax

To enable ORF, run the following command. To return to the default setting, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **capability orf prefix-list** {both| receive| send}

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **capability orf prefix-list** {both| receive| send}

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name

Default value

Non-support

Command mode

BGP configuration mode

Usage guidelines

The command enables BGP to support ORF. ORF is a filtration mode based on prefix-list. It only informs the local required routes to the neighbor, reducing the unnecessary update packets. The command is used by combining with the command "neighbor prefix-list in". The command takes effect only when combining with the command "clear ip bgp *".

Example

The following example shows how to set the output route filtration of neighbor 10.10.10.11(receiving and forwarding):

```
router bgp 100
neighbor 10.10.10.11 remote-as 2
neighbor 10.10.10.11 capability orf prefix-list both
```

Related command

neighbor prefix-list in

clear ip bgp in prefix-filter

6.1.31 neighbor default-originate

Syntax

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the neighbor default-originate command. To send no route as a default, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **default-originate** [route-map *map-name*]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **default-originate**

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
route-map	Set routing attributes with route-map.
map-name	Name of route-map

Default value

No default route is sent to the neighbor.

Command mode

BGP configuration mode

Usage guidelines

Configure this command to send the default route to the neighbor immediately.

This command has nothing to do with whether route 0.0.0.0 is generated in the BGP routing table.

Example

In the following example, The default route will be advertised to the neighbor 160.89.2.3 rather than to 160.89.2.1:

```
router bgp 109
network 160.89.0.0
neighbor 160.89.2.1 remote-as 100
neighbor 160.89.2.3 remote-as 200
```

neighbor 160.89.2.3 default-originate

Related commands

neighbor ebgp-multihop

6.1.32 neighbor description

Syntax

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode. To remove the description, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **description LINE**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **description**

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
line	Text that describes the neighbor.

Default value

There is no description of the neighbor.

Command mode

BGP configuration mode

Usage guidelines

It is easier for user to understand the configuration to associate a description with a neighbor.

Example

In the following example, the description of the neighbor is "peer with abc.com":

router bgp 109

network 160.89.0.0

neighbor 160.89.2.3 description peer with abc.com

6.1.33 neighbor distribute-list

Syntax

Use the **neighbor distribute-list** command to configure the access list to filter the inbound and outbound routes of BGP neighbors. Use no form of the command to delete the configuration:

neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

no neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
access-list name	Name of a standard or extended access list.
In	Access list is applied to incoming advertisements to that neighbor.
Out	Access list is applied to outgoing advertisements to that neighbor.

Default value

none

Command mode

BGP configuration mode

Usage guidelines

One of the methods for neighbor-based filtering BGP route advertisements is to use **neighbor distribute-list**, which uses **access-list** to filter the network prefix information of BGP routes; one method is to use **neighbor filter-list**, which uses aspath-list to filter AS_PATH attribute; another method uses **neighbor prefix-list**, which uses prefix-list to filter the network prefix information.

If you specify a non-existant access list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Example

The following router configuration mode example applies list beijing to incoming advertisements from neighbor120.23.4.1.

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 distribute-list beijing in
```

Related commands

ip aspath-list

neighbor filter-list

ip prefix-list 1

neighbor prefix-list

6.1.34 neighbor ebgp-multihop

Syntax

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ebgp-multihop** *ttl*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ebgp-multihop**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
X:X::X:X	BGP session neighbor IPv6 address.
peer-group-name	BGP peer group name
ttl	Time-to-live in the range from 1 to 255 hops.

Default value

For EBGP-speaking neighbor, only directly connected neighbors are allowed, ttl default value is 1; for IBGP-speaking neighbor, ttl default is 255.

Command mode

BGP configuration mode

Usage guidelines

By default, BGP connection can not be established unless EBGP neighbors are directly connected ones. The allowable maximum number of hops for EBGP neighbors can be set with the **neighbor ebgp-multihop** command.

Ttl is configured to 255 if not specified.

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command.

Example

The following example allows connections to neighbor 131.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109:
neighbor 131.108.1.1 ebgp-multihop
```

Related commands

neighbor default-originate

6.1.35 neighbor fall-over

Syntax

To activate bfd link detection function of the neighbor, run the following command. To return to the default setting, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **fall-over bfd**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **fall-over bfd**

Parameter

Parameter	Description

ip-address	BGP dialogue neighbor IP address
X:X::X:X	BGP dialogue neighbor IPv6 address
peer-group-name	BGP peer group name

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

The command is used to detect the link. If there is problem in the link, bfd will inform bgp to update the route, which will realize fast switch of the route.

Example

none

Related command

neighbor remote-as

bfd enable

6.1.36 neighbor filter-list

Syntax

To configure the as-path list to filter the inbound and outbound routes of BGP neighbors, use the neighbor filter-list command. To disable this function, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

no neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

Parameter

parameter	description

ip-address	IP address of the neighbor.
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
as-path-list name	AS-PATH list name. The ip as-path-list command can be used to define this list.
In	Access list applied to incoming routes.
Out	Access list applied to outgoing routes.

Default value

none

Command mode

BGP configuration mode

Usage guidelines

One of the methods for neighbor-based filtering BGP route advertisements is to use **neighbor distribute-list**, which uses **access-list** to filter the network prefix information of BGP routes; one method is to use **neighbor filter-list**, which uses aspath-list to filter AS_PATH attribute; another method uses **neighbor prefix-list**, which uses prefix-list to filter the network prefix information.

If you specify a non-existant aspath-list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Example

In the following example, the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system AS123:

```
ip as-path-list shanghai deny _123_
ip as-path-list shanghai deny ^123$

router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
neighbor 128.125.1.1 filter-list shanghai out
```

Related commands

ip aspath-list

neighbor distribute-list

ip prefix-list 1

neighbor prefix-list

6.1.37 neighbor maximum-prefix

Syntax

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. To disable this function, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **maximum-prefix** *maximum* [**warnning-only**]

no neighbor {*ip-address* | *X:X::X:X* |*peer-group-name*} **maximum-prefix**

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
Maximum	Maximum number of prefixes allowed from this neighbor.
warnning-only	Only give warning message when the route exceeds the limit.

Default value

This command is disabled by default. There is no limit on the number of prefixes.

Command mode

BGP configuration mode

Usage guidelines

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, the router terminates the peering.

Example

The following example sets the maximum number of prefixes allowed from the neighbor at 129.140.6.6 to 1000:

```
router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 maximum-prefix 1000
```

Related commands

clear ip bgp

6.1.38 neighbor next-hop-self

Syntax

To activate the next-hop processing of BGP updates in the switch and set itself as the next-hop address, use the **neighbor next-hop-self** command. To disable this feature, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **next-hop-self**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **next-hop-self**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
X:X::X:X	BGP session IPv6 address of the neighbor
peer-group-name	BGP peer group name

Default value

This command is disabled by default.

Command mode

BGP configuration mode

Usage guidelines

The disposal of nexthop attribute in BGP is more complicated than IGP. It usually follows three rules:

1. For EBGP session, configure the local ip address of BGP connection as the nexthop attribute when sending routes;

2. For IBGP session, configure the local ip address of BGP connection as the nexthop attribute if the routes are locally generated; if the routes are learned from EBGP, the nexthop attribute is to be filled in intactly the packet when sending routes;

3. If the nexthop parameter of the ip address of the routes belong to the network of BGP session, then the nexthop attribute always adopts the former nexthop;

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Example

The following example forces all updates destined for 131.108.1.1 to advertise this router as the next hop:

```
router bgp 109
neighbor 131.108.1.1 next-hop-self
```

Related commands

set ip next-hop 18

6.1.39 neighbor password

Syntax

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** command. To disable this function, use the no form of this command.

neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **password** *[type] LINE*

no neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **password**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
X:X::X:X	IPv6 address of the neighbor

peer-group-name	BGP peer group name
password	Enables MD5 authentication
type	Password encapsulation type: 0, 6, 7 0 means that the configuration and display are in plain text; 6 indicates that the configuration is in plain text and displayed in cipher text; 7 indicates that the configuration and display are in cipher text Note: The case of not configuring the type is considered as type 0.
LINE	Plainr text password

Default value

none

Command mode

BGP configuration mode

Usage guidelines

Use the neighbor remote-as command to specify the neighbor before using this command.

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The length of password should between 1 and 100 characters(type 7 is 202).

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

Example

The following example configures 'abcd' as the authentication password of neighbor 120.23.4.1:

```
router bgp 109
neighbor 120.23.4.1 remote-as 108
neighbor 120.23.4.1 password abcd
```

Related commands

neighbor remote-as

6.1.40 neighbor peer-group

Use the **neighbor peer-group-name peer-group** command to configure the peer group. Use **no neighbor peer-group-name peer-group** to delete the configured peer group.

Use the **neighbor ip-address peer-group-name** command to configure the neighbor to join the peer group. Use the **no neighbor ip-address peer-group peer-group-name** to delete the neighbor added to the peer group.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

neighbor {*ip-address* **|** *X:X::X:X*} **peer-group** *peer-group-name*

no neighbor {*ip-address* **|** *X:X::X:X*} **peer-group** *peer-group-name*

Parameter

Parameter	Description
ip-address	Neighbor IP address.
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name.

Default

None

Command mode

BGP configuration mode

Usage guidelines

Use the **neighbor peer-group-name peer-group** command to configure the peer group.

Use the **neighbor ip-address peer-group-name** command to configure the neighbor to join the peer group. If there is no configuration on previous neighbor, use this command to configure the peer group's autonomous system number first.

Example

The following example configures a peer group named **group**, and then configures neighbor 10.1.1.1 to join the peer group:

```
router bgp 1
neighbor group peer-group
```

neighbor group remote-as 2
neighbor 10.1.1.1 peer-group group

Related command

neighbor remote-as

6.1.41 neighbor prefix-list

Syntax

To configure prefix-list to filter neighbor routing updates, use the **neighbor prefix-list** command. To remove a filter list, use the no form of this command.

neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

no neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

Parameter

parameter	description
ip-address	IP address of neighbor.
X:X::X:X	Neighbor IPv6 address.
peer-group-name	BGP peer group name
prefix-list	Prefix list is applied to advertisements of that neighbor
prefix-listname	Name of a prefix list.
In	Filter list is applied to incoming advertisements from that neighbor.
Out	Filter list is applied to outgoing advertisements to that neighbor.

Default value

none

Command mode

BGP configuration mode

Usage guidelines

One of the methods for neighbor-based filtering BGP route advertisements is to use **neighbor distribute-list**, which uses **access-list** to filter the network prefix information of BGP routes; one method is to use **neighbor filter-list**, which uses aspath-list to filter AS_PATH attribute; another method uses **neighbor prefix-list**, which uses prefix-list to filter the network prefix information.

If you specify a non-existant prefix-list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Example

The following router configuration mode example applies the prefix list named abc to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list abc in
```

The following router configuration mode example applies the prefix list CustomerA to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list CustomerA in
```

Related commands

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

neighbor filter-list

6.1.42 neighbor remote-as

Syntax

To create a BGP neighbor and specify its autonomous system number, use the neighbor remote-as command in router configuration mode. To the neighbor and all its configurations, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remote-as** *number* [passive]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remote-as** *number*

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name
Number	Nmuber of autonomous system to which the neighbor belongs.
passive	This parameter indicates that the neighbor is configured in passive mode, and will not initiate a TCP connection actively

Default value

none

Command mode

BGP configuration mode

Usage guidelines

The neighbor with the same AS number specified in the **router bgp** command is considered to be IBGP. Otherwise, the neighbor is considered to be EBGP. This command is used to create a neighbor. Only after the neighbor is created, other commands about the neighbor can be configured. If the neighbor has been configurated, you can change its autonomous system number, which will cause the BGP connection to reset.

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command.

Example

In the following example, the local autonomous system is 109, the autonomous systems of neighbors 131.108.200.1, 131.108.234.2, 150.136.64.19 are configured as 167, 109, 99.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

Related commands

neighbor peer-group (creating)

6.1.43 neighbor remove-private-AS

Syntax

To remove private aspath when informing the route to ebgp neighbor, run the following command. To return to the default setting, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remove-private-AS**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **remove-private-AS**

Parameter

Parameter	Description
ip-address	IP address of the neighbor
X:X::X:X	IPv6 address of the neighbor
peer-group-name	BGP peer group name

Default value

None

Command mode

BGP configuration mode

Usage guidelines

None

Example

In the following example, the local autonomous system is 100, the neighbor is 10.1.1.1, 20.1.1.1, the autonomous system is 64512, 200. The command is used to delete private aspath attribute when informing 10.1.1.1 learned route to ebgp neighbor 20.1.1.1.

```
router bgp 100
neighbor 10.1.1.1 remote-as 64512
neighbor 20.1.1.1 remote-as 200
neighbor 20.1.1.1 remove-private-AS
```

Related command

neighbor remote-as

6.1.44 neighbor route-map

Syntax

To apply a ROUTE-MAP to filter the neighbor's inbound and outbound routes, or modify its attributes, use the **neighbor route-map** command. To remove a route map, use the no form of this command.

neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **route-map** *map-name* {*in* **|** *out*}

no neighbor {*ip-address* **|***X:X::X:X* **|** *peer-group-name*} **route-map** *map-name* {*in* **|** *out*}

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
map-name	Name of a route map.
in	Applies route map to incoming routes.
Out	Applies route map to outgoing routes.

Default value

none

Command mode

BGP configuration mode

Usage guidelines

It is only based on neighbor to filter routes using distribute-list, prefix-list and as-path-list, while with route-map, it is not only based on neighbor to filter routes but also based on neighbor to modify the attribute of routes to realize a more flexible routing strategy.

Different routes have different attributes. The route-map can modify attributes of different kinds of routes. If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map. The rules which is valid to BGP route are as follows: match aspath-list, match community-list, match ip address, match ip nexthop, match ip prefix-list, match metric, match tag, set aggregator, set as-path, set atomic-aggregate, set community, set community-additive, set ip nexthop, set local-preference, set metric, set origin, set tag, set weight.

If configured with a non-existent route-map, then all routes is allowed to receive as a result without any modification.

If you specify a BGP or multiprotocol BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Example

The following example applies a route map named internal-map to a BGP incoming route from 198.92.70.24:

```
router bgp 5
neighbor 198.92.70.24 route-map internal-map in
route-map internal-map
match as-path abc
set local-preference 100
```

Related commands

neighbor peer-group (creating)

route-map

6.1.45 neighbor route-reflector-client

Syntax

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command. To indicate that the neighbor is not a client, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **route-reflector-client**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* }| **route-reflector-client**

Parameter

parameter	description
ip-address	IP address of the BGP neighbor being identified as a client.
X:X::X:X	The neighbor’s IPv6 address.

peer-group-name	BGP peer group name.

Default value

There is no route reflector in the autonomous system.

Command mode

BGP configuration mode

Usage guidelines

By default, all internal BGP (iBGP) sessions in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop.

If you use route reflectors, all iBGP sessions need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

Example

In the following example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 198.92.70.24.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
```

Related commands

bgp cluster-id

show ip bgp

6.1.46 neighbor route-refresh

Syntax

To allow neighbor to use route refresh function, use the neighbor route-refresh command. Use the no form of this command to disable route refresh function.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **route-refresh**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **route-refresh**

Parameter

parameter	description
ip-address	BGP neighbor and ip address
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	BGP peer group name.

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

By default, BGP route exchange for only once when the connection is established, then only exchanging changed routes afterwards. If the routing strategy configuration is modified, it will not become effective immediately. Generally, there are two methods:

- Reset BGP connection
- Use soft-reconfiguration function

The first method is relatively slow, and the routes vary greatly. The second method needs too much storage space and occupies more CPU time. These two methods are not good method, and therefore a new method arises, that is, the route refresh.

The route refresh is a negotiation option based on BGP connection, aiming to send the route refresh request packet to ask neighbor to re-send all update packets to oneself, which do not need to reset BGP connection and also do not need to store a great amount of routes. This a a more ideal solution at the moment.

Example

The following example allows neighbor at address 198.92.70.24 to use route refresh function:

```
router bgp 5
neighbor 198.92.70.24 route-refresh
```

Related commands

show ip bgp neighbors

6.1.47 neighbor send-community

Syntax

To specify that a community attribute should be sent to a BGP neighbor, use the neighbor send-community command. To remove the entry, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **send-community** [**standard** | **extended** | **both**]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* }**send-community** [**standard** | **extended** | **both**]

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	BGP peer group name

Default value

The communities attribute can be sent to the neighbor.

Command mode

BGP configuration mode

Usage guidelines

By default, community attributes are not allowed to be sent to neighbors. **Neighbor send-community** command can be used to send routes with community attributes to neighbors.

Use the **show ip bgp neighbors** command to see whether allows to send group attribute to neigh or not.

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command.

Example

In the following example, the switch belongs to autonomous system 109 and is configured to send the COMMUNITIES and EXTCOMMUNITIES attributes to the neighbor at IP address 198.92.70.23:

router bgp 109
no neighbor 198.92.70.23 send-community both

Related commands

match community-list 4

set community 15

set community-additive 17

6.1.48 neighbor send-label

Syntax

To activate neighbor or peer group NLRI with tag, run the following command. To return to the default setting, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **send-label**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* }**send-label**

Parameter

Parameter	Description
ip-address	IP address of neighbor
X:X::X:X	IPv6 address of neighbor
peer-group-name	BGP peer group name

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to activate **nlri** with **mpls** tag, which is usually applied in cross-domain vpn option solution. The command must be combined with command "route-map", if mpls tag is distributed by the public network.

Related command

neighbor remote-as

neighbor route-map

show ip bgp neighbors

6.1.49 neighbor shutdown

Syntax

To disable a neighbor or peer group, use the **neighbor shutdown** command in router configuration mode. To reenable the neighbor or peer group, use the no form of this command.

neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name* } **shutdown**

no neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name* }**shutdown**

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	BGP peer group name

Default value

none

Command mode

BGP configuration mode

Usage guidelines

The **neighbor shutdown** command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

To display a summary of BGP neighbors and peer group connections, use the **show ip bgp summary** or **show ip bgp neighbors** command. Those neighbors with an Idle status and the Admin entry have been disabled by the **neighbor shutdown** command.

Related commands

show ip bgp summary

show ip bgp neighbors

6.1.50 neighbor soft-reconfiguration

Syntax

To configure the software to start storing updates, use the neighbor soft-reconfiguration command in router configuration mode. To not store received updates, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name* } **soft-reconfiguration inbound**

no neighbor {*ip-address*|*X:X::X:X*|*peer-group-name*} **soft-reconfiguration inbound**

Parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	BGP peer group name
inbound	Indicates that the update to be stored is an incoming update.

Default value

The incoming update is not stored and the outgoing update is stored.

Command mode

BGP configuration mode

Usage guidelines

Outbound routing updates will always be stored, and inbound routing updates will only be stored after they are configured. Storing routing updates can take effect without changing the BGP session after changing the routing policy. Resetting the BGP session will bring a lot of network data exchange, and it causes a lot of routing fluctuations. Using soft reconfiguration can avoid a lot of network data exchange and minimize routing fluctuations.

Outbound routing updates are always stored. Inbound routing updates are not stored by default. After changing the local configuration policy, there are three ways to make the new configuration take effect:

First, reset the related BGP session; second, perform local inbound routing soft reconfiguration **clear ip bgp a.b.c.d soft in** (the local switch must be configured with neighbor a.b.c.d soft-reconfiguration); third, the other party performs outbound routing update soft reconfiguration **clear ip bgp a.b.c.d soft out** (no additional configuration required).

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command.

Example

The following example enables inbound soft reconfiguration for the neighbor 131.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy.

```
router bgp 100
neighbor 131.108.1.1 remote-as 200
neighbor 131.108.1.1 soft-reconfiguration inbound
```

Related commands

clear ip bgp

neighbor peer-group (creating)

6.1.51 neighbor timers

Syntax

To set the timers for a specific BGP peer or peer group, use the neighbor timers command in router configuration mode. To clear the timers for a specific BGP peer or peer group, use the no form of this command.

neighbor {*ip-address*|*X:X::X:X*|*peer-group-name}* **timers** keepalive *holdtime* [*Idleholdtime*]

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **timers**

Parameter

parameter	description
ip-address	A BGP peer or peer group IP address.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	Name of the BGP peer group.

Keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer.
Holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead. The range is: 0 or greater than 3
Idleholdtime	The Idleholdtime timer value in seconds

Default value

keepalive: 30 s

holdtime: 90 s

Idleholdtime: 0

Command mode

BGP configuration mode

Usage guidelines

The timer configured for a specific neighbor or peer group overrides the default BGP neighbor timer. Generally, the holdtime is 3 times that of keepalive. If keepalive and holdtime are set to 0, sending keepalive packets is prohibited. At this time, the tcp connection manager need to notify the BGP module that the state of the connection has changed.

Idleholdtime is not 0, which means that the DampPeerOscillation function is activated. When the bgp peer is connected/disconnected 10 times within 5mins, the idleholdtimer is suppressed to keep the bgp peer in the idle state, and the keeping time is the configured idleholdtime.

When Idleholdtime is 0, the DampPeerOscillation function is disabled.

Example

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.98.47.10:

```
router bgp 109
neighbor 192.98.47.10 timers 70 210
```

6.1.52 neighbor ttl-security-hop

To configure TTL hop limit for BGP, run the following command. To return to the default setting, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ttl-security-hop** *value*

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **ttl-security-hop**

Parameter

Parameter	Description
ip-address	IP address of neighbor
X:X::X:X	IPv6 address of neighbor
peer-group-name	peer group name of BGP
value	Value of hop limit. The value ranges from 1 to 254.

Default value

None

Command mode

BGP configuration mode

Usage guidelines

The command is used to configure the max hop supported by bgp neighbor. The connection exceeds this hop cannot be established.

Example

The following example shows how to configure neighbor 10.1.1.2 ttl hop limit to 1:

```
router bgp 100
 neighbor 10.1.1.2 ttl-security-hop 1
```

Related command

neighbor peer-group (creating)

neighbor remote-as

6.1.53 neighbor update-source

To have the software allow Border Gateway Protocol (BGP) sessions to use specified interface for TCP connections, use the **neighbor update-source interface** command. To restore the automatically selected interface, use the no form of this command.

neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **update-source interface**

no neighbor {*ip-address* | *X:X::X:X* | *peer-group-name*} **update-source**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	BGP peer group name
Interface	Interface name

default

Use the local port IP address calculated from the route to establish a TCP connection.

Command mode

BGP configuration mode

Usage guidelines

By default, the ip module decides the local ip address of TCP connection when BGP establishes the connection. IP module decides interface depending on routes, and then binds the main ip address of this interface as the local address of TCP. Use the update-source command can bind the main ip address of the local specified interface during the establishment of TCP connection.

It is generally specified to use loopback interface, for the loopback interface 's protocol state is always up. And so this keeps the stability of BGP session and avoids route fluctuation.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

Example

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface:

```
router bgp 110
network 160.89.0.0
neighbor 160.89.2.3 remote-as 110
neighbor 160.89.2.3 update-source Loopback0
```

Related commands

neighbor peer-group (creating)

6.1.54 neighbor weight

Syntax

To assign a weight to a neighbor connection, use the **neighbor weight** command. To remove a weight assignment, use the no form of this command.

neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **weight** *weight*

no neighbor {*ip-address* **|** *X:X::X:X* **|** *peer-group-name*} **weight**

Parameter

parameter	description
ip-address	IP address of the neighbor.
X:X::X:X	The neighbor's IPv6 address.
peer-group-name	BGP peer group name
Weight	Weight to assign. Acceptable values are from 0 to 65535.

Default value

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local switch have a default weight of 32768.

Command mode

BGP configuration mode

Usage guidelines

BGP routing metric is the important standard to choose routes. The default metric of all routes that learned from neighbors is 0. Use **route-map** command to set metric for routes that learned from neighbor.

If you specify a BGP peer group by using the **peer-group-name** argument, all the members of the peer group will inherit the characteristic configured with this command.

Example

The following router configuration mode example sets the weight of all routes learned via 151.23.12.1 to 50:

router bgp 109

neighbor 151.23.12.1 weight 50

Related commands

neighbor peer-group (creating)

set weight 23

6.1.55 network (BGP)

Syntax

To specify the networks to be advertised by the Border Gateway Protocol (BGP), use the network command. To remove an entry from the routing table, use the no form of this command.

network A.B.C.D/n [**route-map** *map-name* **| backdoor**]

no network A.B.C.D/n

parameter

parameter	description
A.B.C.D/n	Network prefix that BGP will advertise
route-map	The specified route map
map-name	Name of the route map
backdoor	Backdoor network

Default value

No networks are specified.

Command mode

BGP configuration mode

Usage guidelines

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

A totally same route in the main routing table of IP is the basis for the network configured with the network command to become effective.

A more precise or totally same route in the local BTP routing table is the basis for the network to become effective that configured with the **aggretgate-address** command.

The length of mask code is generated in term of standard network type if not specified

Use the route-map to configure route's attribute.

The backdoor network is used to modify route distance rather than to generate routes. It changes route's default distance that learned from the neighbor to the local route's distance. The default value is 200.

The maximum number of network commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

Example

The following example sets up network 131.108.0.0/8 to be included in the BGP updates:

```
router bgp 120
network 131.108.0.0/8
```

Related commands

redistribute (BGP)

aggregate-address

6.1.56 redistribute(BGP)

Syntax

To redistribute a route process to Border Gateway Protocol (BGP), use the redistribute command. To remove the redistribute command from the configuration file, use the no form of this command.

redistribute protocol *process-id*][**route-map** *map-name*] [**metric** *value*]

no redistribute protocol *process-id*

Parameter

parameter	description
protocol	Type of routing protocol
process-id	Process id of routing protocol, such as process if of ospf
route-map	Applies route map to configure route attribute
map-name	Name of route map
metric	Redistribution routing Mertic
value	Metric value. The range is from 0 to 4294967295.

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

Use redistribute command to include routes dynamically to BGP. The change of route source will be reflected to BGP automatically. The automatically-included routes will be informed to other neighbors. The configuration of the redistribute command will re-check the specified type of routes in the routing table. The outer routes in OSPF will not be included to BGP.

Use the **route-map** to configure route's attribute.

Example

The following example configures routes from OSPF process 23 to be redistributed into BGP:

```
router bgp 109
redistribute ospf 23
```

related commands

route-map 1

6.1.57 router bgp

Syntax

To enable the BGP routing process or enter in BGP configuration mode, use the router bgp command in global configuration mode. To disable a routing process, use the no form of this command.

router bgp *as-number*

no router bgp *as-number*

Parameter

parameter	description
as-number	Number of autonomous system

Default value

No BGP routing process is enabled by default.

Command mode

Global configuration mode

Usage guidelines

The system allows to configure one BGP process at most. The BGP task is established in the process of system initialization, and it is activated when the BGP process is started up. The BGP task only receives information from command module without configuring the BGP process. It is not related to routing module or any other module and will not response other information. The related show and clear command are all invalid.

Use no router bgp command to delete BGP process, and at the same time other configuration related to BGP will also be deleted, such as neighbors and so on. The BGP route in routing table is also be deleted.

To configure BGP process using the **show running** and **show ip bgp summary** commands to check.

Example

The following example configures a BGP process for autonomous system 200:

router bgp 200

Related commands

neighbor remote-as

6.1.58 show ip bgp

Syntax

To display entries in the Border Gateway Protocol (BGP) routing table, use the show ip bgp command in user EXEC or privileged EXEC mode.

show ip bgp [**network**]

Parameter

parameter	description
network	Displays the specified routing information

Command mode

EXEC

Usage guidelines

The **show ip bgp** command is used to display the entire IPv4 BGP routing table. After specifying a network, only the detailed information of the network is displayed.

Example

The following is a group of BGP displaying information. The former two lines display some marked information.

Status code indicates the status of the table entry. The status is displayed at the beginning of each line in the table. S indicates the table entry is suppressed, which is the invalid route and will not be chosen. D indicates the table entry is dampened, which is the invalid route. H indicates the table entry history, which is not a ture route and is the invalid route. "* "indicates the table entry is valid, which can be chosen as the best route. " > "indiates the table entry is the best entry to use for that network. "I" indicates the table entry was learned via an internal BGP (iBGP) session.

Origin codes indicates the origin of the entry. I is the entry originated from an Interior Gateway Protocol (IGP). E is the entry originated from an Exterior Gateway Protocol (EGP). ? is the origin of the path is not clear.

For each route, display its status, destination address, gateway address, metric (MED), Local-preference, Weight, AS Path and other attributes. The gateway address of the locally generated route is 0.0.0.0. **Metric** is not displayed if it is not set. Local-preference is 100 by default for IBGP routes, and the default value is included if it is not displayed, or the set value is displayed. **Weight** is 32768 for locally generated routes, or 0 if not set. The **AS Path** field displays the AS Path attribute of the route, including the AS list and the Origin attribute. Enclosed in parentheses are AS-set or AS autonomous sub-systems.

The last line displays number of routes, including all valid and invalid routes.

```
B3710_118#show ip bgp
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network Next Hop Metric LocPrf Weight Path
* 192.168.10.0/24 192.168.69.5 0 10 400 i
*>i192.168.10.0/24 192.168.69.14 100 0 (65030) 400 i
*>i192.168.11.0/24 192.168.69.14 100 0 (65030) 400 i
* 192.168.65.0/30 192.168.69.1 100 0 (65020) 10 ?
*> 192.168.65.0/30 192.168.69.5 0 10 ?
* 192.168.65.4/30 192.168.69.1 100 0 (65020) 10 ?
*> 192.168.65.4/30 192.168.69.5 0 10 ?
* 192.168.65.8/30 192.168.69.1 100 0 (65020) 10 ?
*> 192.168.65.8/30 192.168.69.5 0 10 ?
* 192.168.66.0/30 192.168.66.2 100 0 (65020) ?
*> 192.168.66.0/30 0.0.0.0 32768 ?
* i192.168.66.4/30 192.168.66.6 100 0 ?
*> 192.168.66.4/30 0.0.0.0 32768 ?
*>i192.168.66.8/30 192.168.66.6 100 0 ?
*>i192.168.67.0/30 192.168.69.18 200 100 0 500 ?

Number of displayed routes: 15
```

Related commands

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

6.1.59 show ip bgp community

Syntax

To display statistics of BGP community structure, use the **show ip bgp community** command.

show ip bgp community

Parameter

none

Command mode

exec

Usage guidelines

This command is used to display statistics information of BGP communities attribute structure in the system.

Related commands

show ip bgp

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

6.1.60 show ip bgp ipv6 unicast

Syntax

To show the entry in ipv6 BGP routing table, run the following command.

show ip bgp ipv6 unicast[**network**]

Parameter

Parameter	Description
network	Show the designated routing information.

Command mode

Exec

Usage guidelines

The whole ipv6 BGP routing table is shown if the network is not designated. Details of the network is only shown if the network is designated.

Example

The following is display information of a group of BGP. The front two rows show some tag information.

Status code describes definition of the tag in front of the route. S represents suppression, which indicates the route is suppressed by the aggregation configuration and is an invalid route which will not be selected; d represents attenuation, which indicates the route is suppressed by the fluctuation and is an invalid route; h represents the historic route, which represents the route is saved as of the attenuation control and there is no a real route but only an invalid route. * represents a valid route, which indicates the route is valid and can be selected as the best route; > represents the best route, which indicates the best route slected from the valid routes; I represents the inner route, which indicates the route is from IBGP neighbor, which does not include routes from the sub-autonomous system of the autonomous league.

Origin codes describes the Origin of the route, i means IGP, e means EGP, ? means indefinite.

The command shows the attributes including the status, destination addres, gateway address, Metric(MED), Local-preference, Weight and AS Path of every route. The gateway address of the local route is 0.0.0.0. Metric is not shown if it is not configured with a definite setting. Local-preference for IBGP route is 100 by default; it includes the default value even if it is not shown or it is shown with the set value. Weight is 32768 or the set value; if it is not configured, it is 0. AS Path domain shows the attribute of AS Path, including AS list an Origin attribute. In the brackets is AS-set or sub-autonomous system of the autonomous system league.

The last row shows the number of routes shown altogether, including valid and invalid routes.

Related command

None

6.1.61 show ip bgp neighbors

Syntax

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the show ip bgp neighbors command.

show ip bgp neighbors [*ip-address*] [**received-routes | routes | advertised-routes**]

Parameter

parameter	description
ip-ddress	IP address of a neighbor. If this parameter is omitted, information about all neighbors is displayed.
received-routes	Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	Displays all routes that are received and accepted.
advertised-routes	Displays all routes that have been advertised to neighbors.

Command mode

EXEC

Usage guidelines

With this command, you can see detailed information and current status of neighbors, and you can also see some configuration information. By specifying the corresponding keywords, you can display the routes related to the neighbor.

Related commands

show ip bgp

show ip bgp community

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

6.1.62 show ip bgp paths

Syntax

To display all the BGP paths in the database, use the show ip bgp paths command.

show ip bgp paths

Parameter

none

Command mode

EXEC

Usage guidelines

This command is used to display statistics information of BGP paths structure.

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

6.1.63 show ip bgp prefix-list

Syntax

To display ipv4 BGP routing information matching the specified prefix-list, use the **show ip bgp prefix-list** command.

show ip bgp prefix-list {*prefix-list name*}

Parameter

parameter	description
prefix-list name	Name of prefix-list

Command mode

EXEC

Usage guidelines

This command specifies prefix-list to filter display of the show ip bgp command. Only the routes matching the prefix-list will be displayed.

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

6.1.64 show ip bgp regexp

Syntax

To display routes matching the autonomous system path regular expression, use the show ip bgp regexp command.

show ip bgp regexp *regular-expression*

Parameter

parameter	description
regular-expression	Regular expression to match the BGP autonomous system paths.

Command mode

EXEC

Usage guidelines

This command specifies the regular expression to filter the display of the show ip bgp command. Only the routes matching the regular expression will be displayed.

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

6.1.65 show ip bgp summary

Syntax

To display the status of all Border Gateway Protocol (BGP) connections, use the show ip bgp summary command.

show ip bgp summary

Parameter

This command has no parameters or keywords.

Command mode

EXEC

Usage guidelines

Some global configurations about the BGP protocol can be viewed through the **show ip bgp summary** command. Such as global **distance** configuration, **IGP** synchronization configuration, autonomous system alliance identification number, autonomous system alliance member, route reflection cluster identification, etc. In addition, the local autonomous system number, local router-id, and general information of all neighbors can also be seen through this command.

Example

The following is sample output from the show **ip bgp summary** command:

```
router bgp 4
BGP local AS is 4
Router ID is 192.168.20.72
IGP synchronization is enabled
Distance: external 20 internal 200

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/Pref
192.168.20.12 4 5 0 0 0 0 0 never Connect
```

Related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

6.1.66 synchronization

Syntax

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the **synchronization** command. Use the no form of this command to disable this function.

synchronization

no synchronization

Parameter

none

Default value

Disabled

Command mode

BGP configuration mode

Usage guidelines

IGP synchronization means that when BGP receives a route from IBGP, whether it needs to wait until the route appears in the routing table in the form of IGP before advertising the route to other EBGP neighbors. When IGP synchronization is enabled, BGP must wait until the IBGP route appears in IGP to advertise to other EBGP neighbors; when IGP synchronization is not disabled, BGP will advertise to other EBGP neighbors when it receives IBGP routes. The IGP includes direct routes, static routes, RIP routes, OSPF routes, and other internal gateways protocol routing.

IGP function is disabled by default.

Example

The following example enables switch to advertise the ibgp route after waiting for IGP synchronization.

```
router bgp 120
synchronization
```

Related commands

router bgp

6.1.67 table-map

Syntax

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command. To disable this function, use the no form of the command.

table-map <*name*>

no table-map

Parameter

parameter	description
name	Route map name from the route-map command.

Default value

none

Command mode

BGP configuration mode

Usage guidelines

By setting the table-map, you can filter or modify attributes when BGP adds entries to the routing table.

Example

none

Related commands

none

6.1.68 timers

Syntax

To modify the default timers of BGP neighbors,, use the timers bgp command. To reset the BGP timing defaults, use the no form of this command.

timers bgp <*keepalive*> <*holdtime*> [*Idleholdtime*]

no timers bgp

Parameter

parameter	description
keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer.
holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead.
Idleholdtime	Default Idlehold interval of BGP neighbor

Default value

Keepalive: 30 seconds

Holdtime: 90 seconds

Idleholdtime: 0

Command mode

BGP configuration mode

Usage guidelines

Configure BGP neighbor clock in global configuration mode to modify default clock configuration. The configuration towards neighbor is prior to global configuration.

Example

The following example changes the keepalive timer to 10 seconds and the hold-time timer to 40 seconds:

```
router bgp 100
timers bgp 10 40
```

Related commands

neighbor timers

Chapter 7 Public Routing Configuration Commands

7.1 Ip aspath-list Configuration Commands

7.1.1 ip as-path access-list

Syntax

To create the as-path list, run **ip as-path access-list**. To cancel the configured as-path list, run **no ip as-path access-list**.

ip as-path access-list <*name*> <**deny | permit**> <*regexp*>

no ip as-path access-list <*name*> [**deny | permit**] [*regexp*]

Parameter

Parameter	Description
name	Name of the as-path list
deny | permit	Attribute of the as-path list
regexp	Regular expression of the as-path

Default value

All as-path expressions except those having a clear explanation on the **permit** regulation are declined by default.

Command mode

Global configuration mode

Usage guidelines

The AS-path list is used to filter the AS-PATH attribute of the BGP route. The AS-PATH attribute of the BGP route is a number sequence which is expressed in form of the character string. The number at the right end is the autonomous system number for the route starting, while the numbers leftwards in turn are the numbers of the autonomous systems which the BGP route passes. For example, character string 22 23 98 means that the BGP route is transmitted from autonomous system 98, passes through autonomous system 23 and autonomous system 22, and finally reaches the local autonomous system.

The AS-path list in the system is identified with the name. The total number of AS-path lists which are allowed to configure in the system is limited by the resource of the system. The same AS-path list can be configured with multiple matchup regulation. The procedure to apply the AS-path list is to check whether the matchup is successful or not according to the configuration order. Once a matchup is found to be successful, the following check-up will be stopped and the nature of the regulation (deny/permit) is then returned. If the matchup of all regulations is not successful, the nature of the regulation, **deny**, will be returned. Each regulation is organized according to their configuration order.

The as-path expression is normally the regular expression. The special characters which are always used in the expression are shown in the following table:

Character	Symbol	Meaning
Full stop	.	Matches any single character, including space.
Asterisk	*	Matches the **0** sequence or more sequences.
Plus	+	Matches the **1** sequence or more sequences.
Question mark	!	Follows the number 0 or 1.
Addition character	^	Starting point of the matchup character string
Dollar	$	End point of the matchup character string
Underline	_	Matches these symbols: “”, “{ }”, “( )”, “^”, “$” and “space”.
Square bracket	[ ]	Stands for the range of the single-character mode.
Hyphen	-	Separates a range.

With the aid of the presentation methods of the AS-PATH attribute, the correct usage of the regular expression can help create the powerful AS-path list. The following examples are given:

.* Representing any attribute of the AS path.

^$ Representing the attributes of the null path.

^22$ Representing the path attributes of autonomous system 22.

^22_ Representing the path attribute starting with 22.

_22$ Representing the path attribute starting with 22, such as 22, 34 22 and 99 45 22.

_22_ R epresenting the path attribute containing 22, like 23 22 45 and 442 22 23 44

The **as-path list** command can be used together with the **match as-path** command and the **neighbor filter-list** command.

Example

In the following example, the defined **as-path list hell** command permits all path attributes starting with 23 or containing 22:

ip as-path access-list hell permit ^23

ip as-path access-list hell permit _22_

Or:

ip as-path access-list guangzhou deny ^300

ip as-path access-list guangzhou deny _300_

ip as-path access-list guangzhou permit .*

The AS-PATH attributes starting with 300 or containing 300 will be declined, while other AS-PATH attributes can pass. If the defined order is different, the results will be totally different. The following AS-PATH attributes can pass.

ip as-path access-list guangzhou permit .*

ip as-path access-list guangzhou deny ^300

ip as-path access-list guangzhou deny _300_

Related command

match as-path

neighbor filter-list

7.1.2 show ip aspath-list

Syntax

To display the AS-path list configured in the system, run the following command:

show ip as-path-list [*name*]

Parameter

Parameter	Description
name	Name of the as-path list

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the as-path list is not designated, all configured as-path lists in the system will be displayed.

Example

The following example shows that all as-path lists in the system will be displayed:

show ip as-path-list

Related command

ip as-path access-list

7.2 ip community-list Configuration Commands

7.2.1 ip community-list

Syntax

To create the regulations for the community list of the BGP route, run **ip community list**. To cancel the regulations for the community list, run **no community list**.

ip community-list {**expanded** | **standard**} <*name*> {**deny** | **permit**} [**aa:nn** | *1-4294967295* | **local-AS** | **no-advertise** | **no-export**]

no ip community-list {**expanded** | **standard**} <*name*> {**deny** | **permit**} [**aa:nn** | *1-4294967295* | **local-AS** | **no-advertise** | **no-export**]

Parameter

Parameter	Description
name	Name of the community list
deny | permit	Attribute of the community list
<1-4294967295>	Value of the community, which is a 32-bit integer
aa:nn	New form of the community value **aa** stands for a 16-bit value. **nn** stands for the next 16-bit value.
no-advertise	Means that no neighbor will be reported.
local-AS	Means that the EBGP neighbor outside of the local autonomous system or in the same autonomous system ally will not be reported.
no-export	Means that the neighbors in the local autonomous system or the autonomous system ally will not be reported.

Default value

All communities except those having a clear explanation on the **permit** regulation are declined by default.

Command mode

Global configuration mode

Usage guidelines

The community list is used to filter or set the community attribute of the BGP route. The community attribute is a group number or a community group number. A community number is a 4-byte value. The community numbers between 0x00000000 and 0x0000FFFF or between 0xFFFF0000 and 0xFFFFFFFF are reserved. These community numbers are globally accepted. The frequently-used community numbers are the following ones:

NO_EXPORT (0xFFFFFF01): After the route with this community number is received, the peers outside the autonomous system or autonomous system ally will not be reported.

NO_ADVERTISE(0xFFFFFF02): After the route with the community number is received, no peers will be reported.

NO_EXPORT_SUBCONFED (0xFFFFFF03): It is always called as LOCAL_AS. After the route with the community number is received, the peers outside the local autonomous system are not reported.

The community list in the system is identified by a name. The total number of the community lists which can be configured in the system is limited by the system's resource. The same community list can be configured with multiple matchup regulations. The procedure to apply the community list is to check whether the matchup is successful or not according to the configuration order. Once a matchup is found to be successful, the following check-up will be stopped and the nature of the regulation (deny/permit) is then returned. If the matchup of all regulations is not successful, the nature of the regulation, **deny**, will be returned. The order to check each regulation is the configuration order.

One community-list regulation has three elements: name, regulation's attribute (deny/permit) and community number sequence. The community number sequence is a set of a group of community numbers. If all community numbers in the community attribute are in the community sequence with designated regulations, the matchup is successful. If not, the matchup fails and the next regulation will be matched.

The **community list** command can be used together with commands **route-map** and **match community**.

Example

In the following example, the community will be declined by the **ip community-list yall** command if the value of the community is 5 or 10; the community will be accepted by the **ip community-list yall** command if the value of the community is 15 or 20.

```
ip community-list standard yall deny 5 10
ip community-list standard permit 15 20
```

Related command

match community-list 4

7.2.2 show ip community-list

Syntax

To display the community list configured in the system, run the following command:

show ip community-list <*name*>

Parameter

Parameter	Description
name	Name of the community list

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the community list is not designated, all configured community lists in the system will be displayed.

Example

The following example shows that all community lists in the system will be displayed:

Show ip community-list

Related command

ip community-list

7.3 ip prefix-list commands

7.3.1 clear ip prefix-list

Syntax

To delete the statistics information about the designated prefix list, run the following command:

clear ip prefix-list [<name> [<*prefix*>]]

Parameter

Parameter	Description
name	Name of the prefix list
prefix	Network prefix which is in the A.B.C.D/n format **n** here stands for the length of the mask.

Default

None

Command mode

EXEC

Usage guidelines

If the prefix is not designated, all statistics information in the prefix list will be canceled.

Example

None

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

7.3.2 ip prefix-list

Syntax

To establish a prefix list or add a prefix-list regulation, run **ip prefix-list**. To cancel the configuration, run **no ip prefix-list**.

ip prefix-list <*name*> [<**seq**> <*seq_number*>] <**deny | permit**> <**prefix | any**> [<*ge*> <*value*>] [<**le**> <*value*>]

no ip prefix-list <*name*> [<**seq**> <*seq_number*>] <**deny | permit**> <**prefix | any**> [<*ge*> <*value*>] [<**le**> <*value*>]

Parameter

Parameter	Description
name	Name of the prefix list
seq	Designates the sequence number.
seq_number	Value of the sequence number
deny | permit	Attribute of the prefix list
prefix | any	Designated prefix or any prefix
ge	Designates the minimum length of the matched prefix.
value	Length of the prefix which ranges from 0 to 32
le	Designates the maximum length of the matched prefix.
value	Length of the prefix which ranges from 0 to 32

Default value

None

Command mode

Global configuration mode

Usage guidelines

The prefix list is a set of regulations for filtrating the network prefix. Each regulation has five elements: sequence, deny/permit, prefix and length (a.b.c.d/n), upper limitation (le y) and bottom limitation (ge x). All regulations are sorted according to the sequence. When the prefix list is applied, the regulation of the smallest sequence is first checked. If the matchup is successful, other regulations stop the matchup operation and the matched regulation's attribute (deny/permit) is returned.

When you check whether a regulation matches a designated network prefix, you should not only check the length of the network prefix but also check whether the network prefixes have the same length in the designated length. For example, to check whether a regulation of a prefix list, **ip prefix-list test seq 5 A.B.C.D/M ge X le Y**, matches the designated network **a.b.c.d/n**, the following procedure will be taken.

Firstly, check whether the mask length of the network (n) meets the requirement of the expression: X <= n <= Y (if **ge X** is not designated, the expression is **M <= n<= Y**; if the **le Y** is not designated, the expression is **X <=n <= 32**; if both **ge X** and **le Y** are not designated, the expression is **n** ＝＝ **M**). If the mask length meets the requirements of the expression, the next operation will be performed. If the mask length does not meet the regulation, the following regulation will be used.

Check whether network a.b.c.d/n and the first M bit of A.B.C.D are same. If they are same, the regulation is met and the attribute of the regulation is returned; if the regulation is not met, the next regulation will be seen whether it is met.

If all regulations are not met, the **deny** attribute will be returned.

Regarding the sequence number of the prefix list, there is another command: **ip prefix-list sequence-number**. This command is used to control whether the prefix list uses the sequence number. For details, please refer to the description of this command.

The no form of the command specifying only the name will delete the entire prefix list.

Example

The following are destination routes and prefix lists:

Destination route 1: 120.120.0.0/14

Destination route 2: 120.120.0.0/16

Destination route 3: 120.120.0.0/25

Destination route 4: 130.130.0.0/16

Destination route 5: 130.130.0.0/8

Destination route 6: 130.130.0.0/24

Destination route 7: 12.0.0.0/8

Prefix-list:

ip prefix-list sample permit 120.120.0.0/8 ge 16 le 24

ip prefix-list sample deny 130.130.0.0/16

The following are the matchup results:

Destination route 1: unsuccessful, deny

Destination route 2: successful, permit

Destination route 3: unsuccessful, deny

Destination route 4: successful, deny

Destination route 5: unsuccessful, deny

Destination route 6: unsuccessful, deny

Destination route 7: unsuccessful, deny

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

7.3.3 ip prefix-list description

Syntax

To configure the description of the prefix list, run **ip prefix-list**. To cancel the description of the prefix list, run **no ip prefix-list .**

ip prefix-list <*name*> <**description**> <*strings*>

no ip prefix-list <*name*> <**description**>

Parameter

Parameter	Description
name	Name of the prefix list
description	Designates the description information of the prefix list.
strings	Description information

Default value

None

Command mode

Global configuration mode

Usage guidelines

None

Example

The following example shows how to add the description information to **prefix-list hard** for convenient reading:

ip prefix-list hard deny any

ip prefix-list hard description This prefix-list is used to filter routes from neighbor hard

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

7.3.4 ip prefix-list sequence-number

Syntax

To enable the prefix list to use the sequence, run **ip prefix-list *sequence-number***. To cancel the sequence, run **no ip prefix-list *sequence-number***.

ip prefix-list sequence-number

no ip prefix-list sequence-number

Parameter

None

Default value

The sequence is used by default.

Command mode

Global configuration mode

Usage guidelines

The command is used to decide whether each regulation of the prefix list has been allocated with a sequence. After the sequence is used, the same sequence corresponds to only one regulation. Hence, if a regulation with a same sequence is newly generated, the previously old regulation will be deleted. If the sequence is not used, you have to run a command to delete the regulation. The sequence may not be designated during configuration. The system then allocates the sequence for all regulations. The sequence starts from 5 and adds 5 each time.

Example

None

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

7.3.5 show ip prefix-list

Syntax

To display the information about the prefix list or all prefix lists, including the configuration information and statistics information about the prefix list, run the following command:

show ip prefix-list [<**summary | detail**> <*name*>]

Parameter

Parameter	Description
summary	Summary information
detail	Detailed information
name	Name of the prefix list

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the prefix list is not designated, all information about the prefix list will be displayed.

Example

The following example shows that a prefix list is configured.

ip prefix-list yell permit 130.12.19.0/24

ip prefix-list yell permit 140.20.0.0/16 ge 16 le 24

The following information is shown after the **show ip prefix-list detail** command is run:

Prefix-list with the last deletion/insertion: yell

ip prefix-list yell: 2 entries

count: 2, range entries: 1, sequences: 5 - 10

seq 5 permit 130.12.19.0/24 (hit count: 0, refcount: 10)

seq 10 permit 140.20.0.0/16 ge 16 le 24 (hit count: 0, refcount: 10)

The first information line indicates that the recently-modified prefix list is **yell**.

Starting from the second information line, all information about the prefix list is listed. Here only one prefix list is configured, whose name is **yell**.

Count: 2, indicating that the prefix list has two options.

Range entries: 1, indicating that the number of network range defined in the prefix list is 1.

Sequences: 5-10, indicating the sequence range of each option in the prefix list

The following are the definition of each option and the statistics information.

Hit count: 0, indicating that the times of option matchup is 0

Refcount: 10, meaning that the times of option matchup are 10

Related command

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

7.4 route-map Commands

7.4.1 route-map

Syntax

To create a route map or define a route-map item, run **route-map**. To delete the created route map or the defined route-map item, run **no route-map .**

route-map *name* [*seq*] [**deny** | **permi**]

no route-map *name* [*seq*] [**deny** | **permi**]

Parameter

Parameter	Description
name	Name of the route map
seq	Sequence of the route map whose default value is 0
deny | permit	Attribute of the route map whose default value is **permit**

Default value

By default, the value of the **seq** parameter is 10 and the attribute is **permit**.

Command mode

Global configuration mode

Usage guidelines

The route map is used to modify the route's attribute or the filtration route. The route map is always used for the strategy of the dynamic routing protocol, such as redistribute route, filtration route, setting the route's attribute for strategic routing, and so on.

The same route map may have multiple items. The total number of the route map in the system is limited by the system's resource. Each item in the same route map can be designated with the sequence or the system will automatically generate the sequence for each item. Each item has a kind of attribute (deny/permit); each item can be conducted with the matchup regulation (match), regulations (set) and exit strategies (on-match).

Tue matchup regulation is used to check whether a feature of an object meets a certain rule. If the object meets all matchup regulations in the item, the object matches the item successfully, or the item matchup fails. If an item is not configured with the matchup regulation, any object cannot match the item. If the matchup regulation adopts other lists such as the access list, prefix list, community list or as-path list to check whether an object is matched, the returned value of the list is the result of regulation matchup.

The setting regulation is used to set an attribute of an object. If an object matches the item successfully and the attribute of the item is **permit**, the setting regulations configured under the item are used to modify the attribute of the object. If the object matches the item and the attribute of the item is **deny**, the exit strategy will be checked. If the object fails to match the item, the next item matchup will be conducted until the matchup succeeds.

The exit strategy decides the actions after the object matches the item successfully. If an object matches an item successfully and the item have not configured with the exit strategy, the checking to other items will be stopped and the attribute of the item (deny/permit) will be returned. If **on-match next** is configured, the checking on the next item will be continued. If **on-match goto N** is configured, the designated item, item N, will be the first one to be checked; if the designated item does not exist, the attribute of the item (deny/permit) will be returned.

Under the same item, only one matchup regulation of the same attribute or the settings regulation can be configured. The following matchup regulation or settings regulation configured will replace the previous one. The following configuration can be done for the same item:

match metric 34

set metric 100

In the previous example, there is only one **match** regulation and the **set** regulation.

To realize multiple values for matching the same attribute, you can use the exit regulations.

```
route-map match-multi-metric 10 permit
match metric 10
on-match goto 30
route-map match-multi-metric 20 permit
match metric 20
on-match goto 30
route-map match-multi-metric 30 permit
set metric 100
```

In the same example, the route whose metric is 10 or 20 is matched and its metric will be set to 100.

During configuration, the system can automatically generate a sequence for each item, starting from 10 by default and then adding 10 in turn. When the route map is applied, the system will check the sequence of the item from small to big.

The route map can handle different types of routes, some **match** regulations and **set** regulations only suitable for parts of routes. If you try to use the unsupported **match** regulations or **set** regulations to match or modify the objects, the system will omit these regulations.

If there is no name behind the **no route map** command, the whole route map will be deleted, or the designated item will be deleted.

Example

The following example shows the route map is used to filter the routes forwarded by OSPF and to set the relative attributes.

```
router bgp 20
redistribute ospf 3 route-map redist-ospf
route-map redist-ospf
match tag 139009
set local-preference 300
```

Related command

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.2 match as-path

Syntax

To set a **match** regulation of the route map and check the attributes of the BGP route through the AS-path map, run **match as-path**. To delete the configuration you have just done, run **no match as-path**.

match as-path <*as-path-list-name*>

no match as-path <*as-path-list-name*>

Parameter

Parameter	Description
as-path-list-name	Name of the as-path list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The designated AS path list is used to match the object or to filter the AS-PATH attribute of the BGP route.

Example

The following example shows how to check the whether the BGP route is matched using **as-list1**.

```
route-map match-aspath
match as-path as-list1
```

Related command

route-map

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.3 match community

Syntax

To set a **match** regulation of the route map and check the attributes of the BGP route through the community list, run **match community**. To delete the configuration you have just done, run **no match community**.

match community <*community-list-name*>

no match community <*community-list-name*>

Parameter

Parameter	Description
community-list-name	Name of the community list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The designated community list is used to match the object and to filter the community attribute of the BGP route.

Example

The following example shows how to check the whether the BGP route is matched using **as-list1**.

```
route-map match-comm
match community comm-list1
```

Related command

route-map

match as-path

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.4 match ip address

Syntax

To set a route-map **match** regulation and match the destination network's address, run **match ip address**. To delete the configuration you have just done, run **no match ip address**.

match ip address <*name*>

no match ip address <*name*>

Parameter

Parameter	Description
name	Name of the IP access list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The access list is used to filter the network address of the route, which is suitable for all IP routes and packets.

Example

In the following example, the route checked by the access list is set to metric.

```
route-map set-metric
match ip address acl-metric
set metric 100
```

Related command

route-map

match as-path

match community-list

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.5 match ip next-hop

Syntax

To set a route-map **match** regulation and check whether the next hop address of the route matches with the address of the designated next hop, run **match ip next-hop <*a.b.c.d*>**. To delete the configuration you have just done, run **no match ip next-hop <*a.b.c.d*>**.

match ip next-hop <_a.b.c.d_**>**

no match ip next-hop <*a.b.c.d*>

Parameter

Parameter	Description
a.b.c.d	IP address

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The access list is used to check the attribute of the next hop, which is suitable for all IP routes.

Example

In the following example, the route with the next hop's address 192.121.13.28 matches item 20 of the route map.

```
route-map beijing 10 permit
match ip nexthop 172.12.29.98
set metric 100
route-map beijing 20 permit
match ip nexthop 192.121.13.28
set metric 20
```

Related command

route-map

match as-path

match community-list

match ip address

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.6 match ip address prefix-list

Syntax

To set a route-map **match** regulation and match the destination network's address, run **match ip address prefix list**. To delete the configuration you have just done, run **no match ip address prefix-list**.

match ip address prefix-list <*name***>**

no match ip address prefix-list <*name***>**

Parameter

Parameter	Description
name	Name of the prefix list

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes.

Example

The following example shows that the route whose destination address is 192.121.0.0 matches **route-map match-prefix**.

ip prefix-list beijing permit 192.121.0.0/16

route-map match-prefix

match ip address prefix-list beijing

set metric 100

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.7 match length

Syntax

To set a route-map **match** regulation and check whether the route's metric matches the address of the designated metric, run **match length**. To delete the configuration you have just done, run **no match length**.

match length <*minimum-length*> <*maximum-length*>

no match length <*minimum-length*> <*maximum-length*>

Parameter

Parameter	Description
minimum-length	Minimum length of the packet
maximum-length	Maximum length of the packet

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route.

Related command

route-map

7.4.8 match metric

Syntax

To set a route-map **match** regulation and check whether the route's metric matches the address of the designated metric, run **match metric <*value*>**. To delete the configuration you have just done, run **no match metric <*value*>**.

match metric <_value_>

no match metric <_value_>

Parameter

Parameter	Description
value	Metric value

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all routes.

Example

The following example shows that the routes whose metric values are 120 are declined because they match item 20 of the route map.

```
route-map beijing 10 permit
match ip nexthop 172.12.29.98
set metric 100
route-map beijing 20 deny
match metric 120
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.9 match tag

Syntax

To set a route-map **match** regulation and check whether the route's tag matches the designated tag, run **match tag <*value*>.** To delete the configuration you have just done, run **no match tag <*value*>**.

match tag <*value*>

no match tag <*value*>

Parameter

Parameter	Description
value	Value of the Tag

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all routes.

Example

The following example shows that the routes whose tags' values are 120923 are declined because they match item 20 of the route map.

```
route-map huang 10 permit
match ip nexthop 172.12.29.98
set metric 100
route-map huang 20 deny
match tag 120923
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.10 on-match

Syntax

To configure the exit strategy of the route-map item, run **on-match**. To cancel the configuration, run **no on-match**.

on-match {**next | goto** *n*}

no on-match {**next | goto** }

Parameter

Parameter	Description
n	Sequence of the item

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

The command is used to configure the exit strategy of the route-map item. If a route-map item is successfully matched and the item have not configured with the exit strategy, the checking to other items will be stopped and the attribute of the item (deny/permit) will be returned. If **on-match next** is configured, the checking on the next item will be continued. If **on-match goto N** is configured, the designated item, item N, will be the first one to be checked; if the designated item does not exist, the attribute of the item (deny/permit) will be returned.

Example

None

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.11 set aggregator

Syntax

To configure a route-map setting regulation and set the BGP route to **aggregator**, run **set aggregator**. To delete the configuration you have just done, run **no set aggregator**.

set aggregator as <*as-number*> <*a.b.c.d*>

no set aggregator as <*as-number*> <*a.b.c.d*>

Parameter

Parameter	Description
as-number	Number of the autonomous system of the route aggregator
a.b.c.d	IP address of the route aggregator

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route.

Example

The following example shows that all routes are set to **aggregator**.

```
route-map huang
set aggregator as 200 192.12.90.82
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.12 set as-path

Syntax

To configure a route-map setting regulation and add AS before the **as-path** attribute of the BGP route, run **set as-path prepend**. To delete the configuration you have just done, run **no set as-path prepend**.

set as-path prepend <*as*>

no set as-path prepend <*as*>

Parameter

Parameter	Description
prepend	Means that AS is added before the **as-path** attribute.
as	Number of the autonomous system

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route.

Example

In the following example, the length of the **as-path** attribute is added by adding the autonomous system number before the **as-path** attribute for each route and the result of routing choice is herein changed.

```
route-map add-as
set as-path prepend 200 200 200 200
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.13 set atomic-aggregate

Syntax

To configure a route-map setting regulation and set the BGP route to **aggregator**, run **set atomic-aggregate**. To delete the configuration you have just done, run **no set atomic-aggregate**.

set atomic-aggregate

no set atomic-aggregate

Parameter

None

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route. If the aggregation of information loss is generated when a system transmits the route, you need set the route to **atomic-aggregate**.

Example

In the following example, the length of the **as-path** attribute is added by adding the autonomous system number before the **as-path** attribute for each route and the result of routing choice is herein changed.

route-map tee

set atomic-aggregate

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.14 set community

Syntax

To configure a route-map setting regulation and set the BGP route to **community**, run **set community**. To delete the configuration you have just done, run **no set community**.

set community <*aa:nn* | *1-4294967295* | **local-AS | no-advertise | no-export**>

no set community <*aa:nn* | *1-4294967295* | **local-AS | no-advertise | no-export**>

Parameter

Parameter	Description
aa:nn	Format of the community value
1-4294967295	Value range of the **community** parameter
no-advertise	Means that any neighbor will not be reported.
local-AS	Means that the EBGP neighbor outside of the local autonomous system or in the same autonomous system ally will not be reported.
no-export	Means that the neighbors in the local autonomous system or the autonomous system ally will not be reported.

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route. The newly-set community attribute will replace the previous community attribute of the route.

Example

In the following example, all routes from neighbor 193.12.202.12 will be set to **local-AS community**, enabling these routes not to be reported to other autonomous systems.

```
router bgp 200
neighbor 193.12.202.12 remote 100
neighbor 193.12.202.12 route-map tee in
route-map tee
set community local-AS
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.15 set community-additive

Syntax

To configure a route-map setting regulation and add a value to the community attribute of the BGP route, run **set community-additive**. To delete the configuration you have just done, run **no set community-additive** <*aa:nn* | *1-4294967295* | **local-AS | no-advertise | no-export**>.

set community-additive <*aa:nn* | *1-4294967295* | **local-AS | no-advertise | no-export**>

no set community-additive <*aa:nn* | *1-4294967295* | **local-AS | no-advertise | no-export**>

Parameter

Parameter	Description
aa:nn	Format of the community value
1-4294967295	Value of the **community** parameter
no-advertise	Means that any neighbor will not be reported.
local-AS	Means that the EBGP neighbor outside of the local autonomous system or in the same autonomous system ally will not be reported.
no-export	Means that the neighbors in the local autonomous system or the autonomous system ally will not be reported.

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route. The newly-set community attribute will be added to the previous community attribute of the route.

Example

In the following example, all routes from neighbor 193.12.202.12 will be set to **local-AS community**, enabling these routes not to be reported to other autonomous systems.

```
router bgp 200
neighbor 193.12.202.12 remote 100
neighbor 193.12.202.12 route-map tee in
route-map tee
set community-additive local-AS
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.16 set default

Syntax

To set the default information for the strategy route, run **set default interface**. To cancel the configuration, run **no set default interface**.

set default interface <*interface-name*> [load-balance]

no set default interface <*interface-name*> [load-balance]

Parameter

Parameter	Description
interface-name	Name of the designated interface
load-balance	Allow port routing balance

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. The default outgoing interface of the strategy route is configured through the command. Only when the interface is in the **use** state can this command validate. The interface must meet two conditions before it is used.

Firstly:The UP protocol is running on the interface.

Second: The interface has the IP address or the negotiation IP address, or the interface is the NULL interface.

Related command

route-map

7.4.17 set interface

Syntax

To set the outgoing interface for the strategy route, run **set interface**. To cancel the configuration, run **no set interface**.

set interface <*interface-name*> [load-balance]

no set interface <*interface-name*> [load-balance]

Parameter

Parameter	Description
interface-name	Name of the designated interface
load-balance	Allow port routing balance

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. The default outgoing interface of the strategy route is configured through the command. Only when the interface is in the **use** state can this command validate. The interface must satisfy two conditions before it is used.

Firstly:The UP protocol is running on the interface.

Secondly: The interface has the IP address or the negotiation IP address, or the interface is the NULL interface.

Related command

route-map

7.4.18 set ip default

Syntax

To set the default next hop for the strategy route, run **set ip default nexthop**. To cancel the configuration, run **no set ip default nexthop**.

set ip default nexthop <*A.B.C.D*> [load-balance]

no set ip default nexthop <*A.B.C.D*> [load-balance]

Parameter

Parameter	Description
A.B.C.D	Gateway’s address
load-balance	Allow route balancing for next hop

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. Only when the next hop arrives can this command be valid.

Example

None

Related command

route-map

7.4.19 set ip precedence

Syntax

To set the precedence for the strategy route, run **set ip precedence <0-7>**. To cancel the configuration, run **no set ip precedence <0-7>**.

set ip precedence <0-7>

no set ip precedence <0-7>

Parameter

Parameter	Description
0-7	Precedence which is set for the packet

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. When the suitable route is found by the strategy route for routing, the precedence can also be set. If the strategy route fails, the precedence cannot be set. The precedence of the IP packet is defined as follows:

routine 0

priority	1
immediate	2
flash	3
flash-override	4
critical	5
internet	6
network	7

Related command

route-map

7.4.20 set ip tos

Syntax

To set the tos for the strategy route, run **set ip tos**. To cancel the configuration, run **no set ip tos**.

set ip tos <0-15>

no set ip tos <0-15>

Parameter

Parameter	Description
0-15	TOS which is set for the packet

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to the strategy route. When the suitable route is found by the strategy route for routing, TOS can also be set. If the strategy route fails, the TOS cannot be set. Different TOS' can be set according to their order or can be set together:

normal	0
min-monestary	1
max-reliability	2
max-throughput	4
min-delay	8

Related command

route-map

7.4.21 set ip next-hop

Syntax

To configure a route-map setting regulation and set the next-hop address of the route, run **set ip next-hop**. To delete the configuration you have just done, run **no set ip next-hop**.

set ip next-hop <*a.b.c.d*> [load-balance]

no set ip next-hop <*a.b.c.d*> [load-balance]

Parameter

Parameter	Description
a.b.c.d	IP address
load-balance	Set port load balancing

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes.

Example

In the following example, the next-hop addresses of all routes from neighbor 193.12.202.12 are set to 193.12.202.1:

```
router bgp 200
neighbor 193.12.202.12 remote 100
neighbor 193.12.202.12 route-map tee in
route-map tee
set ip next-hop 193.12.202.1
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.22 set local-preference

Syntax

To configure a route-map setting regulation and set the local preference of the BGP route, run **set local-preference**. To delete the configuration you have just done, run **no set local-preference**.

set local-preference <*value*>

no set local-preference <*value*>

Parameter

Parameter	Description
value	Value of the local preference

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route.

Example

The following example shows that the route map can set **local-preference** to 200:

```
route-map set-local-pref
set local-preference 200
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set metric

set origin

set tag

set weight

show route-map

7.4.23 set metric

Syntax

To configure a route-map setting regulation and set the metric of the route, run **set metric**. To delete the configuration you have just done, run **no set metric**.

set metric <*value*> [*BEIGRP-delay reliability loading MTU*]

no set metric <*value*> [*BEIGRP-delay reliability loading MTU*]

Parameter

Parameter	Description
value	Value of the metric
BEIGRP-delay	BEIGRP port delay (unit: 10ms). Range is from 0 to 4294967295.
reliability	BEIGRP port reliability (255 means completely reliable). Range is from 0 to 255.
loading	BEIGRP load parameters (255 represents full load). Range is from 0 to 255.

MTU	BEIGRP port MTU. Range is from 0 to 4294967295.

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes.

Example

The following example shows that the route map can set **metric** to 120:

```
route-map set-metric
set metric 120
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set origin

set tag

set weight

show route-map

7.4.24 set metric-type

Syntax

To set the value of the metric-type parameter for supporting the external type OSPF route, run **set metric-type**. To delete the configuration you have just done, run **no set metric-type**.

set metric-type [**type-1** | **type-2**]

no set metric-type [**type-1** | **type-2**]

Parameter

Parameter	Description
Type-1	External type-1 of OSPF metric
Type-2	External type-2 of OSPF metric

Default value

None

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to external OSPF routes.

Example

The following example shows that the route map can set **metric-type** to **type1**:

route-map set-metric-type
set metric-type type-1

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

show route-map

7.4.25 set origin

Syntax

To set the origin attribute of the BGP route, run **set origin**. To delete the configuration you have just done, run **no set origin**.

set origin {**igp** | **egp** | **incomplete**}

no set origin {**igp** | **egp** | **incomplete**}

Parameter

Parameter	Description
igp	Internal route of the autonomous system
egp	External route of the autonomous system
incomplete	Uncertain route

Default value

Igp is he default route locally configured through the **network** command, **Incomplete** is the default route locally configured through the **aggregate** command or the **redistribute** command.

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route.

Example

The following example shows how the defined route map sets the BGP route with a 10-starting **original** attribute to **igp**.

```
ip as-path-list self permit ^10
route-map set-origin
match as-path self
set origin igp
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set tag

set weight

show route-map

7.4.26 set tag

Syntax

To set the tag of the route, run **set tag**. To delete the configuration you have just done, run **no set tag**.

set tag <*value*>

no set tag <*value*>

Parameter

Parameter	Description
value	Value of the tag

Default value

The default tag value is 0.

Command mode

Route-map configuration mode

Usage guidelines

This command is suitable to all IP routes.

Example

The following example shows how to set **tag** to 120980 through the route map:

```
route-map set-tag
set tag 120980
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set weight

show route-map

7.4.27 set weight

Syntax

To set the weight of the BGP route, run **set weight**. To delete the configuration you have just done, run **no set weight**.

set weight <*value*>

no set weight <*value*>

Parameter

Parameter	Description
value	Value of the weight

Default value

The default weight value of the locally-generated BGP route is 32768 and the weight value obtained from the neighbor is 0.

Command mode

Route-map configuration mode

Usage guidelines

This command is only suitable to the BGP route.

Example

The following example shows how to set the weight to 230 through the route map:

```
route-map set-weight
set weight 230
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

show route-map

7.4.28 show route-map

Syntax

To display the information about the route map, run the following command:

show route-map [*name*]

Parameter

Parameter	Description
name	Name of the route map

Default value

None

Command mode

EXEC

Usage guidelines

If the name of the route map is not designated, all configured route maps in the system will be displayed.

Example

The following example shows that all route maps in the system are displayed:

```
Show route-map
```

Related command

route-map

match as-path

match community-list

match ip address

match ip next-hop

match ip prefix-list

match metric

match tag

on-match

set aggregator

set as-path

set atomic-aggregate

set community

set community-additive

set ip next-hop

set local-preference

set metric

set origin

set tag

set weight

Chapter 8 PBR Configuration Commands

8.1 PBR Configuration Commands

HTTP configuration commands include:

- debug ip policy
- ip policy route-map
- match ip address
- match length
- set default interface
- set interface
- set ip default next-hop
- set ip next-hop
- route-map
- Debug ip policy
- ip local policy
- ip policy
- ip route-weight
- show ip local policy
- show ip policy

8.1.1 debug ip policy

Syntax

To check the results of applying the policy route, run **debug ip policy**. To return to the default setting, use the no form of this command.

debug ip policy

no debug ip policy

Parameter

None

Default value

By default, the results of policy route application will not be printed.

Command mode

EXEC

Usage guidelines

This command can be used to check whether the IP packets received from the interface have been applied with the policy route.

Because the results of policy routing application for each interface-received IP packet will be printed after this command is run, please use this command when the network traffic is low.

Example

The following example shows how to display the policy routing debug information

Router# debug ip policy

2004-1-16 15:32:54 PBR: s=10.1.1.2 (vlan1), d=99.1.1.1, len 84, policy rejected -- normal forwarding

2004-1-16 15:32:54 PBR: s=10.1.1.21 (vlan1), d=99.1.1.1 (vlan2), len= 84, gate=13.1.1.99 policy routed

Related command

None

8.1.2 ip policy route-map

Syntax

To apply the policy route to the interface-received IP packet, run **ip policy route-map route-map name** in interface configuration mode. To cancel the policy route on the interface, run **no ip policy route-map**.

ip policy route-map *route-map name*

no ip policy route-map

Parameter

Parameter	Description
route-map name	Name of the route map

Default value

None

Command mode

Interface configuration mode

Usage guidelines

If you want to apply the policy route to the interface-received IP packet, you need to run the **ip policy route-map** command.

Example

The following example shows how to enable the policy route on interface vlan1.

Switch _config#int vlan1
Switch _config_v1#ip policy route-map pbr

Related command

route-map

8.1.3 match ip address

Syntax

To apply the matchup policy based on source IP address, run **match ip address *access-list name***.

match ip address *access-list name*

no match ip address [*access-list name*]

Parameter

Parameter	Description
access-list name	Name of the standard IP access control list

Default value

The access list is not designated by default.

Command mode

Route-map configuration mode

Usage guidelines

If the route map is applied to the policy route, the source address of the IP packet will be used to match the configured access list. If the source address does match the access list, the **set** regulation is then applied; otherwise, the next sequence number of the same route map will be used.

Example

The following example shows that the packets whose source IP addresses are allowed by access list **net1** will be transmitted to interface vlan2:

```
Interface vlan1
ip policy route-map moon
!
route-map moon
match ip address net1
set interface vlan2
```

Related command

set default interface

set interface

set ip default next-hop

set ip next-hop

route-map

8.1.4 match length

Syntax

To set the route policy according to the length of the IP packet, run **match length**.

match length *minimum-length maximum-length*

no match length *minimum-length maximum-length*

Parameter

Parameter	Description
minimum-length	Designates the minimum length of the matched packet.
maximum-length	Designates the maximum length of the matched packet.

Default value

It is not configured by default.

Command mode

Route-map configuration mode

Usage guidelines

This command is used to conduct the policy routing according to the size of the IP packet.

Example

The following example shows that the IP packet whose size ranges between 1000 bytes to 1500 bytes will be transmitted to interface vlan2.

```
Interface vlan1
ip policy route-map moon
!
route-map moon
match length 1000 1500
set interface vlan2
```

Related command

match ip address

set default interface

set interface

set ip default next-hop

set ip next-hop

route-map

8.1.5 set default interface

Syntax

To set the default next-hop interface for the matched IP packet, run **set default interface**.

set default interface *interface name* [*...interface name*] [**load-balance**]

no set default interface *interface name* [*...interface name*] [**load-balance**]

Parameter

Parameter	Description
interface name	Name of the interface

Default value

It is not configured by default.

Command mode

Route-map configuration mode

Usage guidelines

Before you set the default next-hop interface for the matched IP packet through the set default interface command, the following conditions must be satisfied:

(1) The **set ip next-hop** command is not configured, or the **set ip next-hop** command is configured but the route of the next hop designated by **set ip next-hop** is not in the routing table.

(2) If the **set interface** command is not configured or the **set interface** command is configure but these interfaces cannot be routed (the interface is down or there is no IP address).

(3) The **set ip default next-hop** command or the **set ip default next-hop** command is not configured but the route of the next hop designated by **set ip default next-hop** is not in the routing table.

Example

None

Related command

match ip address

match length

set interface

set ip default next-hop

set ip next-hop

route-map

8.1.6 set interface

Syntax

To set the next-hop interface for the matched IP packet, run **set interface**.

set interface interface name [*...interface name*] [**load-balance**]

no set interface interface name [*...interface name*] [**load-balance**]

Parameter

Parameter	Description
interface name	Name of the interface

Default value

It is not configured by default.

Command mode

Route-map configuration mode

Usage guidelines

Before you set the next-hop interface for the matched IP packet through the set interface command, the following conditions must be satisfied:

(1) The **set ip next-hop** command or the **set ip next-hop** command is not configured, and the route of the next hop designated by **set ip next-hop** is not in the routing table.

(2) The interface is in the routing state (the protocol on the interface is up and the IP address exists).

Example

None

Related command

match ip address

match length

set default interface

set ip default next-hop

set ip next-hop

route-map

8.1.7 set ip default next-hop

Syntax

To set the default next-hop for the matched IP packet, run **set ip default next-hop**.

set ip default next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

no set ip default next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

Parameter

Parameter	Description
A.B.C.D	Address of the next hop

Default value

It is not configured by default.

Command mode

Route-map configuration mode

Usage guidelines

Before you set the default next hop for the matched IP packet through the **set ip default next-hop** command, the following conditions must be satisfied.

(1) The **set ip next-hop** command or the **set ip next-hop** command is not configured, and the route of the next hop designated by **set ip next-hop** is not in the routing table.

(2) If the **set interface** command is not configured or the **set interface** command is configure but these interfaces cannot be routed (the interface is down or there is no IP address).

(3) The route of the next hop designated by the **set ip default next-hop** command exists in the routing table.

Related command

set default interface

set interface

set ip next-hop

route-map

8.1.8 set ip next-hop

Syntax

To set the next hop for the matched IP packet, run **set ip next-hop**.

set ip next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

no set ip next-hop *A.B.C.D* [*...A.B.C.D*] [**Load-balance**]

Parameter

Parameter	Description
A.B.C.D	Address of the next hop

Default value

It is not configured by default.

Command mode

Route-map configuration mode

Usage guidelines

Before you set the next hop for the matched IP packet through the **set ip next-hop** command, the following conditions must be satisfied:
The route of the next hop designated by the **set ip next-hop** command exists in the routing table.

Related command

set default interface

set interface

set ip default next-hop

set ip next-hop

route-map

8.1.9 route-map

Syntax

route-map *route-map name* [*sequence-number*] [**permit | deny**]

no route-map *route-map name* [*sequence-number*] [**permit | deny**]

Parameter

Parameter	Description
route-map name	Name of the route map
sequence-number	Sequence number of the designated route map, which is optional
permit	Means that the route or the policy route is allowed to be forwarded if the IP packet is matched. The parameter is optional.
deny	Means that the route or the policy route is forbidden to be forwarded if the IP packet is matched. The parameter is optional.

Default value

There is no static routes by default.

Command mode

Global configuration mode

Usage guidelines

The **route-map** command is used to configure the route map.

Example

The following example shows that route map **pbr** is configured.

```
route-map pbr 10 permit
match ip address net1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address net2
set ip next-hop 14.1.1.99
!
route-map pbr 30 permit
match ip address net3
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
```

Related command

match ip address

match length

set default interface

set interface

set ip default next-hop

set ip next-hop

8.1.10 ip local policy

Syntax

To open the policy route of the local packet, run **ip local policy route-map [*name*]**. To shut down the policy route of the local packet, run **no ip local policy route-map [*name*]**.

ip local policy route-map *name*

no ip local policy route-map *name*

Parameter

Parameter	Description
name	Name of the route map used by the policy route

Default value

The policy routing function of the local packet is shut down by default.

Command mode

Global configuration mode

Usage guidelines

The policy route can be applied to the locally-transmitted packets or the forwarded packets. The route applied to the locally-transmitted packets are called as the local policy route. After the **ip local policy route-map <*name*>** command and a proper route map are configured in global configuration mode, you can apply the policy route to the locally-transmitted packets.

The policy route checks whether the packets are the broadcast packets, and the broadcast packets also checks the corresponding policy route. Among the results of the policy route, only an outgoing interface or a next hop is shown. The route-to-multiport condition does not exist.

The route map which is used for the policy route can match the packet according to the access list or the packet's length. The policy routing is conducted by setting the next hop or the outgoing interface. Various policies can be satisfied using the access list according to the routes, such as the route of the source address and the application route.

The policy route can be used to set the outgoing interface, next hop, TOS and precedence of the packet. The order to choose the policy route is as follows: nexthop, default nexthop, interface and default interface. The normal route can be adopted when all the four types of previous policy routes are unavailable.

If **nexthop** is available, it means that a route can be found in the routing table for **nexthop**. If **interface** is available, it means that the IP protocol on the interface is up and the legal IP address exists.

Example

The following example shows that the policy routing is conducted to the locally-transmitted packets. The packets from the network whose destination address is 100.0.0.0/8 will be transmitted to interface vlan1:

```
ip local policy route-map Policy
!
```

```
route-map Policy
match ip address Policy-ACL
set interface vlan1
!
ip access-list extended Policy-ACL
permit ip any 100.0.0.0 255.0.0.0
!
```

Related command

ip policy

show ip local policy

show ip policy

8.1.11 ip policy

Syntax

To open the policy route on an interface, run **ip policy route-map [*name*]**. To shut down the local policy route, run **no ip policy route-map [*name*]**.

ip policy route-map *name*

no ip policy route-map

Parameter

Parameter	Description
name	Name of the route map used by the policy route

Default value

The policy routing function on an interface is shut down by default.

Command mode

Port configuration mode

Usage guidelines

The policy route can be applied to the locally-transmitted packets or the forwarded packets

The policy route is to check whether the packet is the broadcast packet, while the broadcast packet is also to check the corresponding policy route.

The route map which is used to match the policy route can match the packet according d to the access list or the packet's length. Various policy requirements can be satisfied through the usage of the access list, such as source-address-based routing and application-based routing.

You can set the egress port, nexthop, tos and precedence for the policy route. When the policy route is used, the order to select the route is: set ip nexthop, set interface,non-default normal route, set ip default nexthop, set default interface, normal route or default route. The policy route can set tos and precedence uniquely for normal routes.

The availability of nexthop means that the nexthop can be used to find a route in the routing table. The interface availability means that the IP protocol on the interface is up and the interface has a legal IP address.

Example

The following example shows that the policy routing can be conducted to a packet received by interface vlan1 and the packet whose destination address is 100.0.0.0/8 can be transmitted to interface vlan2:

```
interface vlan1
ip policy route-map Policy
!
route-map Policy
match ip address Policy-ACL
set interface vlan2
!
ip access-list extended Policy-ACL
permit ip any 100.0.0.0 255.0.0.0
!
```

Related command

ip local policy

show ip local policy

show ip policy

8.1.12 ip route-weight

Syntax

To configure the route weight on an interface, run **ip route-weight**. To resume the original route weight on an interface, run **no route-weight**. The original value of the route weight is 1.

ip route-weight [*value*]

no ip route-weight

Parameter

Parameter	Description
value	Route weight

Default value

The default value of the route weight is 1.

Command mode

Port configuration mode

Usage guidelines

You can configure the **ip route-weight** command on an interface to realize rate-based flow distribution.

At first, you need to configure the **ip route load-balance** command in global mode; then, you need to configure the route weight at the egress port of the equivalence route according to the flow distribution rate. In this way, the packet can be transmitted on different egress ports of the equivalence route according to the configured rate. In this case, you must disable the ip cache function.

Example

The following example shows that the packet is transmitted at a rate of 3:2 on interface vlan1 and interface vlan2 after it arrives destination network 5.0.0.0.

```
Interface vlan1
ip route-weight 3
ip address 3.0.0.1 255.0.0.0
no ip directed-broadcast
!
interface vlan2
ip route-weight 2
```

```
ip address 8.0.0.1 255.0.0.0
no ip directed-broadcast
duplex half
!
ip route load-balance
ip route 5.0.0.0 255.0.0.0 FastEthernet0/0 1.2.3.5 2
ip route 5.0.0.0 255.0.0.0 Ethernet1/1 2.2.3.5 2
```

The route weight of interface vlan1 is set to 3, while the route weight of interface vlan2 is set to 2. If they are configured as 6 and 4 respectively, they will have the same effect. Their greatest common divisor is eliminated here

Related command

ip route load-balance

ip route-cache

8.1.13 show ip local policy

Syntax

show ip policy

Parameter

None

Default value

None

Command mode

EXEC mode

Usage guidelines

show ip local policy

The command is used to how to show the configuration status of local policy routing.

Example

None

Related command

ip local policy

ip policy

show ip policy

8.1.14 show ip policy

Syntax

show ip policy

Parameter

None

Default value

None

Command mode

EXEC mode

Usage guidelines

The **show ip policy** command is used to display the configuration state of the policy route.

Example

None

Related command

ip local policy

ip policy

show ip local policy

Chapter 9 Switch Routing Protocol Highpriority Configuration Commands

9.1 Switch Routing Protocol Highpriority Configuration Commands

Switch routing protocol highpriority configuration commands include:

- switch routing-protocol-highpriority

9.1.1 switch routing-protocol-highpriority

Syntax

To enable or disable set priority of the routing packets forwarding to CPU, run the following command. To return to the default setting, use the no form of this command.

[no] switch routing-protocol-highpriority

Parameter

None

Default value

Disabled

Command mode

Global configuration mode

Usage guidelines

None

Example

The following example shows how to set priority of the routing packets forwarding to CPU.

```
Switch _config# switch routing-protocol-highpriority
Switch _config#
```